HACETTEPE ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ

Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

BİLGİ GÜVENLİĞİNE YÖNELİK ÇEVRİMİÇİ EĞİTİMİN ORTAOKUL ÖĞRENCİLERİNİN SANAL ORTAMLARDA BİLGİ GÜVENLİĞİNE İLİŞKİN ÖĞRENMELERİNE ETKİSİ

Fatma GÖLPEK SARI

Doktora Tezi

Ankara, 2021

Liderlik, araştırma, inovasyon, kaliteli eğitim ve değişim ile

Daha ileriye... En İyiye...

HACETTEPE ÜNİVERSİTESİ
EĞİTİM BİLİMLERİ ENSTİTÜSÜ

Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

BİLGİ GÜVENLİĞİNE YÖNELİK ÇEVRİMİÇİ EĞİTİMİN ORTAOKUL ÖĞRENCİLERİNİN SANAL ORTAMLARDA BİLGİ GÜVENLİĞİNE İLİŞKİN ÖĞRENMELERİNE ETKİSİ

THE EFFECT OF INFORMATION SECURITY ONLINE TRAINING ON SECONDARY SCHOOL STUDENTS' INFORMATION SECURITY LEARNING IN ONLINE ENVIRONMENTS

Fatma GÖLPEK SARI

Doktora Tezi

Ankara, 2021

Öz

Bu araştırmanın amacı, çevrimiçi bir ortamda verilen “Sanal Ortamlarda Bilgi Güvenliği” ne yönelik eğitimlerin; ortaokul öğrencilerinin, sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerine etkisinin incelenmesidir. Araştırmada nicel araştırma yöntemlerinden yarı deneysel desen kullanılmış, araştırma nitel verilerle de desteklenmiştir. Araştırmanın çalışma grubunu Ankara ilinde merkezi bir ortaokulda öğrenim görmekte olan ortaokul öğrencileri oluşturmaktadır. Pilot uygulama ve asıl uygulama süreci için farklı çalışma gruplarına başvurulmuş olup pilot uygulama süreci 30, asıl uygulama süreci ise 52 öğrenci ile yürütülmüştür. Araştırmada nicel ve nitel veriler kullanılmıştır. Veri toplama sürecinde; kişisel bilgi formu, sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı ve açık uçlu anket formları kullanılmıştır. Kullanılan istatistiksel yöntemler belirlenirken, öncelikle çalışma gruplarının normal dağılım gösterip göstermediği test edilmiştir. Nicel verilerin analizi için bilgisayar tabanlı bir istatistik programı kullanılmıştır. Nitel verilerin analizi için ise sırasıyla betimsel analiz ve içerik analizi yöntemlerine başvurulmuştur. Araştırmanın sonuçları; öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerinin, bilgi güvenliği hakkında daha önce yüz yüze ya da çevrimiçi eğitim alma durumuna bağlı olarak değişmediğini öte yandan öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerinin tasarlanan ortamdaki eğitimler sonrasında yükseldiğini göstermektedir. Bu durum, tasarlanan ortam aracılığıyla tamamen çevrimiçi ortamda gerçekleştirilen eğitimin başarılı olduğu şeklinde yorumlanabilir. Ayrıca eğitimlerin öğrenilenlerin kalıcılığını sağlama konusunda da etkili olduğu sonucuna ulaşılmıştır. Araştırmanın bir diğer sonucu ise; eş zamansız eğitimlere ek olarak gerçekleştirilen eş zamanlı eğitimlerin; sadece eş zamansız eğitimlere kıyasla öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmeleri ve öğrenilenlerin kalıcılığı açısından bir farklılık oluşturmadığı şeklindedir. Araştırma sonuçları doğrultusunda farklı yaş gruplarına yönelik çevrimiçi eğitimlerin etkililiğine ilişkin deneysel çalışmalar önerilebilir.

Anahtar sözcükler: bilgi güvenliği, çevrimiçi güvenlik, çevrimiçi risk, çevrimiçi güvenlik bilinci, çevrimiçi öğrenme, ortaokul öğrencileri

Abstract

The purpose of this research is examining the effects of the trainings developed for "Information Security in Virtual Environments" given in an online environment, on the learning of secondary school students about information security in virtual environments. Quasi-experimental design was used in the research, and the research was supported by qualitative data. The study group of the research consists of secondary school students in a central secondary school in Ankara. The piloting process 30; the main implementation process was carried out with 52 students. In the data collection process, personal information form, a tool for determining the level of information security in virtual environments and open-ended questionnaires were used. It was tested whether the study groups showed a normal distribution. A computer-based statistical program was used for analyzing quantitative data. Descriptive analysis and content analysis methods were used analyzing qualitative data. The results of the research; that students' learning about information security in virtual environments did not change depending on whether they had received a previous training about information security. The results shows that students' learning about information security increased after the trainings. The trainings are effective in ensuring the permanence of learning. Also synchronous training in addition to asynchronous training; compared to the asynchronous training conducted only in the online environment, there is no difference in terms of the level of information security of the students in virtual environments and the permanence of what has been learned. New experimental studies can be suggested for different age groups.

Keywords: information security, online security, online risk, online safety awareness, online learning, secondary school students

Teşekkür

Doktora sürecimin başından sonuna dek gerek çalışmalarımda gerekse tez yazma sürecinde desteğini esirgemeyen, sabırla bütün sorularıma yanıt veren danışmanım Prof. Dr. Süleyman Sadi SEFEROĞLU'na teşekkürü bir borç bilirim.

Tez yazma sürecinde görüş ve önerileriyle tezime sağladıkları değerli katkıları için TİK üyeleri Prof. Dr. Mukaddes ERDEM ve Prof. Dr. Ebru KILIÇ ÇAKMAK'a şükranlarımı sunarım.

Tez savunma sınavıma katılarak tezime sundukları katkılar için Prof. Dr. Alev ÖZKÖK ve Prof. Dr. Serçin KARATAŞ'a teşekkür ederim.

Tez süreci boyunca sabırla sorularımı yanıtlayan Dr. Öğretim Üyesi Mehmet Fatih YİĞİT'e ve uygulamalarımı yürüttüğüm süreçte sağladığı desteklerinden dolayı Soner UYSAL'a teşekkürü bir borç bilirim.

Gerek doktora ders süreci gerekse tez sürecinde bana ve emeklerime olan inancını yitirmeyen, desteklerini esirgemeyen eşim Emrah SARI'ya sonsuz teşekkürler. Bu süreçte manevi desteğini esirgemeyen babam ve anneme de sonsuz teşekkürler.

Doktora yolculuğumun başından sonuna dek benimle yürüyen oğlum Can ve doktora sürecimin son zamanlarında dünyaya gelen kızım İnci, iyi ki varsınız.

İçindekiler

Tablolar Dizini

Şekiller Dizini

Simgeler ve Kısaltmalar Dizini

ITU: Uluslararası Telekomünikasyon Birliği (International Telecommunication Union)

ARCS: Dikkat, İlgi, Güven, Doyum (Attention, Relevance, Confidence, Satisfaction)

NICCS: ABD Ulusal Siber Güvenlik Kariyer ve Çalışmaları Girişimi (National Initiative For Cybersecurity Careers And Studies)

KGO: Kapsam Geçerlik Oranı

KGİ: Kapsam Geçerlik İndeksi

Bölüm 1.
Giriş

Bu bölümde problem durumu, araştırmanın amacı ve önemi, araştırma problemi, sayıltılar, sınırlılıklar ve tanımlar yer almaktadır.

Problem Durumu

COVID-19 küresel salgın sürecinde eğitimlerin çevrimiçi ortamlar aracılığıyla sürdürülme ihtiyacı; çocukların internette geçirdikleri zamanın artmasına sebep olmuştur. Bu durum birtakım çevrimiçi risk ve tehditleri de beraberinde getirmiştir. Çevrimiçi güvenlik, bilgi güvenliği, e-güvenlik gibi kavramlar yeni olmamakla birlikte teknolojinin hızla gelişmesi sebebiyle bireylerin güvenlik ve risk farkındalıklarının önemi güncelliğini hala korumaktadır.

Bilgi teknolojilerinin hızla geliştiği ve yayıldığı son yıllarda bilgiye erişim yolları artmış, bilgiye erişim kolaylaşmıştır. Erişilen bilgi miktarının da her geçen gün arttığı günümüzde, sıklıkla önemi gündeme gelen konulardan birisi de bilgi güvenliğidir. Bilgi ve iletişim teknolojilerinin benimsenmesi, bir dizi yeni güvenlik açığı ve dolayısıyla kişisel ve örgütsel verilerin gizliliği ve bütünlüğüne yönelik yeni tehditleri beraberinde getirmiştir (Parsons vd., 2017). Bilgi güvenliği ihlallerinin en sık nedeni olarak bilgisayar kullanıcılarının tesadüfi ve bilinçsiz davranışları kabul edilmektedir (Parsons vd., 2015).

Bilgi güvenliği, bilginin tehlikelerden veya tehditlerden korunması için doğru teknolojinin, doğru şekilde ve doğru amaçla kullanılarak, istenmeyen kişiler tarafından elde edilmesini önleme çabası olarak tanımlanmıştır (Sağıroğlu & Alkan, 2018). Bilgi ve iletişim teknolojilerinin hızlı gelişimi ve günlük hayattaki pek çok iş ve işlemin bilgi ve iletişim teknolojileri aracılığıyla yapılması büyük avantajlar sağlasa da zaman zaman çeşitli riskleri de beraberinde getirebilmektedir. Dijital ortamlarda bilgi güvenliğinin sağlanamaması da bu riskler arasında düşünülebilir. Çevrimiçi ortamlarda riskler ve tehditler gerek öğrenciler gerekse yetişkinler açısından ciddi bir sorun haline gelebilmektedir. Seferoğlu, Yıldız-Durak, Karaoğlan-Yılmaz ve Yılmaz (2018) da kişisel ve kurumsal bilgi güvenliğinin sağlanmasının ve bilgi güvenliğiyle ilgili farkındalığın artırılmasının önem kazandığını belirtmiştir. Yine Seferoğlu, Yıldız-Durak, Karaoğlan-Yılmaz ve Yılmaz' a göre, bilgi güvenliğiyle ilgili

olarak temel amaç, kişilerin bilgi ve iletişim teknolojilerini kullanırken tehdit ve tehlikelerin farkına varmalarını ve gerekli önlemleri almalarını sağlamaktır.

Bilgi güvenliği araştırmaları, insan faktörünün bilgi güvenliğinin en zayıf halkası olması sebebiyle insana odaklanmaktadır. Bilgi güvenliği ile ilgili olarak bir kuruluştaki bireylerden ne beklendiğini tanımlamak için güvenlik politikaları kullanılmakla birlikte, kullanıcıların güvenlik politikalarına uymamaları söz konusu olabilmektedir (Tsohou vd., 2015). Bilinçlendirme ya da farkındalık eğitimleri, kullanıcıları güvenlik sorunlarından ve politikalarından haberdar etmeyi hedeflemektedir. Farkındalık eğitimleri; bilinçlendirme ya da farkındalık bilgisinin, gerçekten güvenlik davranışlarının gelişmesine neden olup olmayacağını genellikle dikkate almayabilmektedir (Tsohou vd., 2015). Bu hususta, bilgi güvenliği farkındalığı eğitimlerinin bireylerin kazanımlarına ve davranış değişikliklerine odaklanmasında yarar olacağını söylemek mümkündür. Yine Tsohou vd.'ne göre, bireylerin bilgi güvenliği davranışını nasıl destekleyeceğini anlayabilmek için, bireylerin güvenlik bilinci bilgisini nasıl içselleştirdiğini anlamamız ve güvenlikle ilgili karar vermenin biçimlendirilmesinde önyargıların etkisinin anlaşılması gerekmektedir. Rezgui ve Marks (2008) da yapmış oldukları bir çalışmada, bilinçlilik, kültürel varsayımlar, inançlar ve sosyal koşullar gibi faktörlerin, üniversite personelinin davranışlarını ve özellikle de bilgi güvenliği bilincini etkilediğini ortaya koymaktadır. Kearney ve Kruger (2016) bilgi güvenliği bilincinin risklerin sürekli değişmesi nedeniyle daha da zorlaşan dinamik bir süreç olduğundan bahsetmektedir. Bu doğrultuda herhangi bir farkındalık eğitiminin, risk profillerindeki değişiklikleri takip edebilmek için sürekli olarak ölçülmesi ve yönetilmesi gerektiğini vurgulamaktadır.

Bilgi güvenliği kavramına yönelik bir alanyazın incelemesi yapıldığında; siber güvenlik, siber sağlık, veri güvenliği, internet güvenliği, e-güvenlik ve çevrimiçi güvenlik gibi terimlere rastlanmaktadır (Hartikainen vd., 2019; Mıhçı & Kılıç Çakmak, 2017, Kılınç, 2012; Sağıroğlu & Alkan, 2018). Kişilerin konu olduğu bilgiler "isme bağlı veriler" veya "bireysel veriler" şeklinde ifade edilmektedir (Kılınç, 2012). Başta devlet olmak üzere, çeşitli kamu kuruluşları, özel hukuktaki kâr amaçlı kuruluşlar, sivil toplum kuruluşları kullanıcılardan çeşitli verileri toplamaktadır. Bilgi güvenliği kavramı kapsamında kişisel veri güvenliği, ya da diğer bir tabirle dijital veri güvenliği düşünülebilir. İnternetin hayatımızın her alanına dâhil olduğu, cep telefonlarında pek

çok kişisel verinin depolandığı ve sıklıkla sosyal ağların kullanıldığı göz önünde bulundurularak, bireylerin bilgi güvenliği ve dijital veri güvenliği kavramlarına yönelik bilgi ve farkındalık sahibi olmalarının önemli olduğu söylenebilir. Erol ve Sağıroğlu (2018) farkındalık eğitimlerinin etkili olduğunu, ancak günümüzde siber saldırıların iki eğitim arasında geçen süreden çok daha kısa sürelerde gerçekleşmesi sebebiyle yetersiz kaldığını belirtmektedir. Bu anlamda en etkili yöntemin, farkındalık düzeyinin doğru yöntemlerle ölçülmesi ve modellenerek insanlar tarafından davranışa dönüştürülmesine dayandığını belirtmektedir.

Bilgi güvenliği kavramı siber ortamlar açısından düşünüldüğünde "siber güvenlik" kavramı ön plana çıkmaktadır. Siber güvenlik, "veri, işlem, süreç, politika, deneyim, kapasite, insan ve sistemlerin güvenliğinin siber ortamda sağlanması" şeklinde tanımlanmaktadır (Sağıroğlu ve Alkan, 2018). Uluslararası Telekomünikasyon Birliği'ne göre siber güvenlik; siber ortamı, kullanıcı varlıklarını ve organizasyonu korumak için kullanılabilecek araçlar, güvenlik kavramları, politikalar, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitim, güvence ve teknolojilerin toplamıdır (ITU, 2020).

Bilgi güvenliği konusunda sıklıkla karşılaşılan bir diğer terim de çevrimiçi güvenliktir. Çevrimiçi güvenlik, bir kişinin fiziksel ve psikolojik güvenliğinin yanı sıra itibar, kimlik ve çevrimiçi mülkiyeti, donanım, yazılım, bilgi ve fikri mülkiyet de dahil olmak üzere mülkün korunması olarak tanımlanmıştır (Hartikainen vd., 2019). Alanyazında çevrimiçi güvenlik kavramı çevrimiçi riskler, tehditler ve zarar boyutlarıyla dikkat çekmektedir. Çelen, Çelik ve Seferoğlu (2011) bilgisayar ve internet teknolojilerinin yaygınlaşmasının bilgi edinme, iletişim gibi birçok yönden günlük hayatımıza katkı sağlarken çocuklar ve gençler için tehdit de oluşturmaya başladığını belirtmektedirler. Yine çevrimiçi ortamlarda çocukların; internet üzerinden tehdit, uygun olmayan ve tehlikeli işlere maruz kalma, gizlilik ihlali ve çevrimiçi dolandırıcılık gibi risklere maruz kalabilecekleri vurgulanmaktadırlar. Bu hususta; çocukların ve gençlerin çevrimiçi etkinliklerden olumsuz bir şekilde etkilenmesini önlemek için gerekli düzenlemelerin yanı sıra bilinçlendirme çalışmalarının yürütülmesinin gerekliliği bu çalışmada dikkat çekilen diğer bir durumdur.

Çevrimiçi ortamlar, özellikle çocuklar açısından birtakım riskleri barındırabilmektedir. Çevrimiçi ortamdaki riskler, çocuklar tarafından üzücü veya

zararlı olarak deneyimlenmeyebilmektedir. Livingstone vd. (2011) Avrupa Çevrimiçi Çocuklar (EU Kids Online) projesi kapsamında; çocukların çevrimiçi ortamda karşılaşmış oldukları riskleri belirlemeye yönelik 9-16 yaş aralığındaki çocuklar ve aileleri ile bir çalışma gerçekleştirmişlerdir. Bu proje kapsamında çocukların dijital okuryazarlık ve güvenlik becerileri, interneti aşırı kullanımları, çevrimiçi aktivite sıklıkları, çevrimiçi içeriğin kalitesi, çocukların sosyal ağ kullanımları, çevrimiçi ortamdaki riskler ve zarar deneyimleri konularında araştırma yapılmıştır. Araştırma sonuçları çocukların daha genç yaşlarda çevrimiçi olduklarını; 9-10 yaşındaki çocukların %67'sinin internet hakkında ebeveynlerinden daha fazla şey bilmediklerini söylediklerini göstermiştir. İnternet güvenliği kampanyaları ve girişimlerinin, özellikle ilkokullarda olmak üzere, daha küçük yaş grupları için uyarlanırken, aynı zamanda daha büyük çocuklar için mevcut çabaların sürdürülmesi gerekliliği vurgulanmaktadır. Araştırma kapsamında ayrıca her sekiz çocuktan birinin internette cinsel imajlar görmek ve cinsel mesajlar alma durumu ile karşılaştığı, ancak genellikle bunlara maruz kalan birkaç çocuk dışında bu durumun çocuklar tarafından zararlı olarak görülmediği bulgusuna ulaşılmıştır. Çirkin veya incitici mesajlar alarak çevrimiçi zorbalığa uğramanın nispeten daha nadir gerçekleştiği ve bunun yirmi çocuktan biri tarafından deneyimlendiği, ancak bu durumun çocukları üzme olasılığının en yüksek risk olduğu belirtilmiştir. Yine, 12 çocuktan sadece birinin çevrimiçi bir kişiyle çevrimdışı tanıştığı ve çocuklara göre bu riskin nadiren zararlı olduğu sonucuna ulaşılmıştır. Öğretmenler ve diğer eğitimcilerin, dijital beceriler ve e-güvenlik eğitimi için önemli sorumluluk taşıdıkları ve bu rolü yerine getirmek için desteklenmeleri gerektiği belirtilmiştir (Livingstone vd., 2011). Bu bilgiler doğrultusunda, çevrimiçi ortamdaki risklerin meydana getirebileceği zararlı sonuçlar konusunda çocukların bilgilendirilmesinin önemli olduğu söylenebilir.

Smahel vd. (2020) Avrupa Çevrimiçi Çocuklar (EU Kids Online) projesi kapsamında; daha önce yapılmış olan araştırma kapsamını genişletmiş, 2010 yılında elde edilen verileri 2020 yılında elde edilen verilerle kıyaslamışlardır. Bu kapsamda; bazı ülkelerde çocukların her gün çevrimiçi olarak geçirdiği sürenin 2010 yılına kıyasla neredeyse iki kat arttığı bilgisine ulaşılmıştır. Çocukların çoğunun ebeveynlerinden, öğretmenlerinden veya arkadaşlarından herhangi bir çevrimiçi güvenlik tavsiyesi almadıkları, çevrimiçi ortamda olumsuz deneyimin, yaşla birlikte

arttığı araştırmanın diğer bulguları arasındadır. Çevrimiçi ortamda olumsuz deneyime sahip çocukların benzer deneyimleri birkaç kez yaşadıkları; bu gibi olumsuz deneyimler karşısında birisi ile paylaşmanın yanı sıra; uygulama veya pencereyi kapatmak, sorunu görmezden gelmek veya kişiyi engellemek gibi davranışlar sergiledikleri raporlanmıştır.

Sosyal medyanın ve diğer ağ teknolojilerinin yaygın olarak benimsenmesi, çocukların çevrimiçi olduklarında karşılaştıkları tehditler hakkında endişelere yol açmaktadır (Boyd & Hargittai, 2013). Okullarda dijital öğrenmeyi, dijital katılımı ve dijital okuryazarlığı teşvik etmek için birçok ülkede farklı politikalar ve eğitim çabaları bulunmaktadır (Ólafsson vd., 2013). Avrupa Birliği düzeyinde, "Daha Güvenli İnternet Programı ve "Çocuklar İçin Daha İyi Bir İnternet için Avrupa Stratejisi" girişimi buna örnek olarak gösterilebilir. "Çocuklar İçin Daha İyi Bir İnternet İçin Avrupa Stratejisi" girişimindeki amaç, çocuklara çevrimiçi ortamdan güvenli bir şekilde yararlanmak için ihtiyaç duydukları becerileri kazandırmaktır. Bu amaçla Avrupa Komisyonu, ulusal eğitim sistemlerinin çevrimiçi güvenlik konularına nasıl yaklaştığını ve çocukların okullarda çevrimiçi güvenlik hakkında ne öğrendiklerini belirlemeye çalışmaktadır (Hartikainen vd., 2019). Çevrimiçi mahremiyet becerilerine yönelik de özellikle ortaokul ve lise düzeyinde birçok eğitim programının geliştirildiği görülmektedir (Common Sense Media, 2021; International Computer Science Institute, 2021; Office of the Privacy Commissioner of Canada, 2019; Raynes-Goldie & Allen, 2014).

Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine yönelik farkındalık sahibi olmaları önemli bir konudur. Ortaokul öğrencilerine yönelik olarak yapılmış bir çalışmada, siber sağlık çatısı altında ortaokul öğrencilerine yönelik internet bağımlılığı, çevrimiçi nezaket, çevrimiçi mahremiyet, siber zorbalık, çevrimiçi uygunsuz içerik, telif hakkı ve çevrimiçi güvenlik ölçekleri geliştirilmiştir. Siber sağlık çatı kavramının genel olarak "bireyin kendine ve diğerlerine saygısı, güvenli ve sorumlu kullanım" olmak üzere iki ilke çerçevesinde tanımlandığı belirtilmiştir (Mıhçı ve Kılıç Çakmak, 2017). İlk ilke olan bireyin kendine ve diğerlerine saygısı ilkesi, çevrimiçi öğrencilerin kendi itibarını koruması ve diğerlerine saygı göstermesine yönelik davranışları içermektedir. İkinci ilke olan güvenli ve sorumlu kullanım ilkesi ise öğrencilerin zararlı ve yasadışı çevrimiçi davranışların sonuçlarını anlamasına odaklanmıştır (Mıhçı & Kılıç Çakmak, 2017).

Bilgiye erişimin belirli mekân ve zamanla kısıtlanamayacağı gerçeğinden hareketle çevrimiçi öğrenme konusunun incelenmesinde yarar olduğu düşünülmektedir. Çevrimiçi öğrenmeye yönelik yaygın olarak kullanılan terimler arasında e-öğrenme, ağa bağlı öğrenme, sanal öğrenme, bilgisayar destekli öğrenme, web tabanlı öğrenme ve uzaktan eğitim yer alır. Khan (1997) çevrimiçi eğitimi, Web'i ortam olarak kullanarak uzak bir kitleye eğitim vermek için yenilikçi bir yaklaşım olarak tanımlamaktadır. Ally (2008) ise çevrimiçi öğrenmeyi, "öğrenme materyallerine erişmek için internet kullanımı; içerik, eğitmen ve diğer öğrencilerle etkileşimde bulunmak; öğrenme süreci boyunca, bilgi edinmek, kişisel anlam oluşturmak ve öğrenme deneyiminden destek almak" şeklinde tanımlamaktadır.

Çevrimiçi ortamdaki riskler ve tehditler göz önüne alındığında, öğrencilere yönelik tasarlanmış bir çevrimiçi ortamda yürütülen eğitimlerin öğrencilerin sanal ortamlarda bilgi güvenliği düzeyleri ve farkındalığı açısından katkı sağlayabileceği düşünülebilir. Alanyazında ebeveynler ve akranları genellikle çocukların çevrimiçi güvenliğinde önemli aktörler olarak tanımlanmaktadır (Hasebrink, vd., 2011). Okullarda dijital teknolojilerin kullanımı arttıkça, öğretmenler de çocukları korurken internet kullanımlarını nasıl teşvik edecekleri sorusuyla karşı karşıyadır (Ahn vd., 2011). Bununla birlikte, çocukların çevrimiçi güvenliğini başkalarının eylemlerine bağlı bir şey olarak görmenin yanı sıra, çevrimiçi güvenlik çocukların bağımsızlıkları ve gelişimsel süreçleri ile etkinleşen bir eylem olarak da görülebilir (Hartikainen vd., 2019; Wisniewski vd., 2014). Mıhçı ve Kılıç Çakmak (2017) da internette sorumlu ve güvenli davranışlar sergilemenin önemine yönelik eğitim sağlamanın önemli olduğunu belirtmektedirler. Yine öğrencilerin internet kullanımını sadece okul saatlerinde kontrol etmenin yetersiz olduğunu, onların interneti her nerede olursa olsun belirli bir sorumluluk çerçevesinde kullanabilme bilincine ulaşmasının büyük oranda eğitim ile sağlanabileceğini ifade etmektedirler.

Küresel salgın koşulları sürecinde, eğitimlerin devam ettirilebilmesi amacıyla çevrimiçi ortamlara sıklıkla başvurulmuştur. Çevrimiçi kursların veya derslerin etkililiğinin sağlanması için etkileşim önem arz etmektedir. Mabrito'ya göre (2006) herhangi bir etkileşimli çevrimiçi kursta eğitmen-öğrenci ve öğrenci-öğrenci etkileşimi temel özellik olmalıdır. Teknolojik gelişmeler, öğretmenlerin aynı zamanlı uygulamaları kullanarak öğrencileriyle derslerini gerçekleştirebilmesine olanak sağlamaktadır. Küresel salgın koşullarında da farklı öğretim kademelerinde aynı

zamanlı araçlar, eğitmen- öğrenen etkileşimini sağlamada oldukça önemli bir rol oynamıştır. Çevrimiçi ortamlarda eş zamanlı dersler uzun yıllardır kullanılmakla birlikte, ilkokul ve ortaokul öğrencilerinin kullanımının son birkaç yılda yaygınlaştığını söylemek mümkündür. Özellikle aynı zamanlı ders uygulamalarının önemine yönelik alanyazında son yıllarda pek çok çalışmaya rastlanmaktadır (Lapitan vd., 2021; Reinholz vd., 2020; Wang & Wang, 2021; Wang vd., 2018; Weiler, 2012;). Örneğin Wang vd. (2018) yapmış oldukları çalışmada, öğrencilerin harmanlanmış aynı zamanlı öğrenme ortamının tasarımı ve uygulamasına ilişkin ne tür öğrenme deneyimleri ve

algıları olduğunu araştırmışlardır. Çalışma sonuçları yüz yüze öğretimin özelliklerinin bir kısmının çevrimiçi öğrenenler için de geçerli olduğunu göstermiştir. Öğrenciler, uzak yerlerde video konferans yoluyla derslere katılmanın esnekliğini ve rahatlığını vurgulamışlardır.

Küçük yaşlardan itibaren internet ortamında zaman geçiren öğrencilerin, sanal ortamlarda bilgi güvenliği hakkında bilgi ve farkındalık sahibi olmalarının önemli olduğu düşünülmektedir. Özellikle küresel salgın koşullarında çevrimiçi ortamlarda eğitimlere sıklıkla başvurulması, çevrimiçi ortamlarda yürütülen eğitimlerin etkililiğini tekrar gündeme getirmektedir. Ortaokul öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmeleri belirlenerek bilgi güvenliğine yönelik geliştirilen çevrimiçi ortamda eğitim planlamasının yapılması ve eğitimin etkililiğinin araştırılması, incelenmesi gereken bir konu olarak değerlendirilmektedir. Yine ortaokul öğrencilerine yönelik olarak çevrimiçi ortamda eş zamanlı (aynı zamanlı) ve eş zamansız (ayrı zamanlı) derslerin etkililiği açısından bir değerlendirmenin de incelenmesi gereken bir diğer konu olduğu düşünülmektedir.

Araştırmanın Amacı ve Önemi

Bu araştırmanın amacı, çevrimiçi bir ortamda verilen “Sanal Ortamlarda Bilgi Güvenliği” ne yönelik olarak geliştirilmiş eğitimlerin; ortaokul öğrencilerinin, sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerine etkisinin incelenmesidir. Bu çalışmanın diğer bir amacı çevrimiçi ortamda yürütülen eğitimlerin öğrenilenlerin kalıcılığına etkisinin araştırılmasıdır. Yine; çevrimiçi ortamda eş zamansız eğitimlere katılan öğrenciler ile çevrimiçi ortamda eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliği düzeyleri ve

öğrenilenlerin kalıcılığı arasında bir ilişki olup olmadığının belirlenmesi de çalışmanın bir diğer amacıdır.

Bilgi güvenliği günümüzde sadece yetişkinleri değil aynı zamanda çocukları da ilgilendiren bir konu haline gelmiştir. Çocukların çevrimiçi ortamlarda geçirdiği zaman ve karşılaştıkları riskler göz önüne alındığında sanal ortamlarda bilgi güvenliği eğitimlerinin çocuklar için ne kadar gerekli ve önemli olduğu daha iyi anlaşılabilir. Okullar, ebeveynler tarafından internet güvenliği bilgileri hakkında en güvenilir bilgi kaynağı olarak kabul edilmektedirler. Öğretmenlerin ve diğer eğitimcilerin, dijital beceriler ve e-güvenlik eğitimi için önemli sorumluluk taşıdıkları ve bu rolü yerine getirmek için desteklenmeleri gerektiği belirtilmektedir (Livingstone vd., 2011). Zilka (2017) da çevrimiçi gizlilik, siber zorbalık, şiddet barındıran içeriğe maruz kalma, dışlanma ve nefreti körükleyen içeriğe maruz kalma, yabancılarla çevrimiçi iletişim ve kaba dil kullanımı gibi unsurları içeren güvenliğin önemli bir sorun haline geldiğini belirtmiştir.

Beder ve Ergün (2015) ortaokul öğrencilerinin güvenli internet kullanım durumlarını araştırdıkları çalışmasında, ortaokul öğrencilerinin bilinç seviyelerinin artırılabilmesi için, çocukları güvenli internet kullanımı ile ilgili bilinçlendirmeye yönelik eğitsel çalışmaların planlanması önerisinde bulunmuşlardır. Gökçearslan ve Seferoğlu (2016) da ortaokul öğrencilerinin internet kullanım biçimlerini araştırdıkları çalışmalarında; öğrencilere, ailelere ve çeşitli kurumlara çevrimiçi riskler konusunda sorumluluk düştüğünü, paydaşların işbirliği ile sorunların çözülebileceğini belirtmişlerdir.

Günümüzde öğrencilerin çevrimiçi ortamlardan sıklıkla faydalanması, çevrimiçi ortamların zaman planlaması, eğitmen desteği, geribildirim ihtiyacı, bireysel farklılıklar vb. unsurları gözetebilmesi, güvenilir ve güncel kaynaklara olan ihtiyaçları düşünüldüğünde; bilgi güvenliği eğitimine yönelik bir çevrimiçi ortam tasarımının gerçekleştirilmesinin ve eğitimlerin yürütülmesinin öğrencilerin sanal ortamlardaki bilgi güvenliği düzeyleri açısından katkı sağlayabileceği düşünülmektedir. Alanyazında bilgi güvenliği eğitimine yönelik gerçekleştirilen araştırmaların çalışma gruplarını genellikle lise ve yükseköğretim öğrencileri ile yetişkinlerin oluşturduğu görülmektedir. Oysa bilgi güvenliği günümüzde çocukları da ilgilendiren bir konu haline gelmiştir. Bu anlamda bu çalışmada; ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliği düzeylerini belirleyebilmek amacıyla

araştırmacı tarafından bir değerlendirme aracı geliştirilmiş; sanal ortamlarda bilgi güvenliği eğitimine yönelik çevrimiçi bir ortam tasarlanmış ve bu ortamda yürütülen eğitimlerin öğrencilerin bilgi güvenliği düzeylerine etkisi araştırılmıştır. Böylelikle bu çalışmanın, ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliği davranışlarını geliştirmeye yönelik gerek alanyazın gerekse uygulama açısından katkı sağlaması beklenmektedir.

Alanyazında bilgi güvenliği eğitimine yönelik gerçekleştirilen çalışmalarda genellikle yüz yüze yürütülen eğitimlerin etkililiğinin araştırıldığı, çevrimiçi ortamlarda yürütülen bilgi güvenliği eğitimlerinin etkililiğine yönelik çalışmaların sınırlı sayıda olduğu görülmektedir. Bu açıdan bakıldığında da bu çalışmanın sanal ortamlarda bilgi güvenliğine yönelik geliştirilen bir çevrimiçi ortam aracılığıyla verilen eğitimlerin etkililiğini belirleyebilmek adına alanyazın ve uygulama açısından katkı sağlayacağı düşünülmektedir.

Öğrenilenlerin kalıcılığına yönelik alanyazında pek çok çalışmaya rastlanmakla birlikte, bilgi güvenliği eğitimlerinin kalıcılığına yönelik herhangi bir çalışmaya rastlanamamıştır. Oysa bilgi güvenliği eğitimleri sonucunda öğrenilenlerin farklı zamanlarda tekrar sınanması gerekliliği önemli bir konudur. Bu çalışmanın sanal ortamlarda bilgi güvenliğine yönelik eğitimlerin kalıcılığını belirleyebilmek adına alanyazın ve uygulamaya katkı getirebileceğine inanılmaktadır.

Çevrimiçi ortamlarda aynı zamanlı ve ayrı zamanlı tekniklerin uygulamasına yönelik alanyazında pek çok çalışmaya rastlanmaktadır. Gerek aynı zamanlı gerekse ayrı zamanlı teknikler kendi içerisinde birtakım avantajları ve sınırlılıkları barındırmaktadır. Özelikle aynı zamanlı tekniklerin öğrenci-öğrenci ve öğrenci-eğitmen etkileşimi açısından avantajlı bulunması gerçeğinden hareketle bu çalışmada çevrimiçi ortamda ayrı zamanlı eğitimlere katılan öğrenciler ile çevrimiçi ortamda ayrı zamanlı eğitimlere ek olarak aynı zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliği düzeyleri ile öğrenilenlerin kalıcılığı arasındaki bir ilişki olup olmadığı araştırılarak alanyazın ve uygulama açısından katkı sağlanmaya çalışılmıştır.

Genel olarak özetlemek gerekirse bu çalışmanın; sanal ortamlarda bilgi güvenliği eğitimine yönelik geliştirilen çevrimiçi bir ortamda yürütülen eğitimlerin

ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliği düzeylerine etkisini belirlemeyi amaçlaması sebebiyle özgün ve alanyazına katkı sağlayacak bir çalışma olduğu söylenebilir. Çevrimiçi ortamda yürütülen eğitimlerin öğrenilenlerin kalıcılığına etkisinin araştırılması, çevrimiçi ortamda ayrı zamanlı eğitimlere katılan öğrenciler ile çevrimiçi ortamda ayrı zamanlı eğitimlere ek olarak aynı zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliği düzeyleri ve öğrenilenlerin kalıcılığı arasındaki bir ilişki olup olmadığının araştırılmasının da bu çalışmanın özgün ve alanyazına katkı sağlayacak bir çalışma olarak yorumlanabileceğini düşündürmektedir.

Araştırma Problemi

Bu çalışmanın araştırma problemi "Sanal ortamlarda bilgi güvenliği eğitimine yönelik olarak geliştirilmiş bir çevrimiçi ortamda yürütülen eğitimlerin, ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerine etkisi nedir?" şeklindedir. Bu problem çerçevesinde aşağıdaki alt problemlere yanıt aranmıştır.

Alt problemler

1. Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri nedir?
2. Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri, bilgi güvenliği hakkında daha önce yüz yüze ortamda bir eğitim alma durumuna göre nasıl değişmektedir?
3. Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri, bilgi güvenliği hakkında daha önce çevrimiçi ortamda bir eğitim alma durumuna göre nasıl değişmektedir?
4. Sanal ortamlarda bilgi güvenliği ile ilgili eğitime yönelik tasarlanan ortamda yürütülen eğitimlerin ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliği ile ilgili bilgi durumlarındaki değişimine etkisi nedir?
5. Çevrimiçi ortamda yürütülen bilgi güvenliği ile ilgili eğitimlerin öğrenilenlerin kalıcılığına etkisi nedir?
6. Çevrimiçi ortamda eş zamansız eğitimlere katılan ortaokul öğrencileri ile eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin

sanal ortamlarda bilgi güvenliğine yönelik öğrenmeleri açısından istatistiksel olarak anlamlı bir fark var mıdır?

7. Çevrimiçi ortamda eş zamansız eğitimlere katılan öğrenciler ile eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliğine yönelik öğrenilenlerin kalıcılığı açısından istatistiksel olarak anlamlı bir fark var mıdır?
8. Sanal ortamlarda bilgi güvenliği ile ilgili olarak çevrimiçi ortamda yürütülen eğitimlere katılan öğrencilerin aldıkları eğitime yönelik görüşleri nelerdir?

Sayıltılar

Bu araştırma aşağıdaki sayıltılara dayalı olarak yürütülmüştür:

Araştırmanın uygulama sürecindeki yönlendirmelerin tüm katılımcıları benzer şekilde etkilediği varsayılmaktadır.

Sınırlılıklar

Bu araştırma aşağıdaki sınırlılıklar kapsamında yürütülmüştür:

Katılımcıların farklı çevrimiçi araçları kullanımı, geliştirilen çevrimiçi ortamdaki iletişim araçlarının kullanımını sınırlandırabilmiştir.

Araştırma kapsamında yürütülen uygulamaların aynı zamanlı dersler boyutu, olağan koşullarda okullarda yüz yüze derslerde yürütülecekken, COVID-19 salgın sürecinde çevrimiçi ortamda video konferans aracı ile yürütülmek zorunda kalınmıştır. Bu durum, etkileşimi sınırlandırabilmiştir.

Avantajlar

Yüz yüze eğitimin yapıldığı deneysel çalışmalarda, araştırmaya katılan gruplar arasındaki etkileşimi kontrol edebilmek çok mümkün olmayabilmektedir. Bu araştırmada; deneysel süreç tamamen çevrimiçi ortamda yürütüldüğünden, gruplar arası etkileşimin olağan koşullarda okullarda yüz yüze yürütülen derslerdeki etkileşime kıyasla daha az gerçekleştiği söylenebilir. Bu durum, araştırmanın bir avantajı olarak düşünülebilir.

Tanımlar

Bilgi Güvenliği: Bir varlık türü olarak kabul edilen bilginin başkaları tarafından izinsiz ya da yetkisiz bir şekilde erişilmesini, kullanılması, değiştirilmesini, herkese açık olarak paylaşılmasını, yok edilmesini, başkalarına verilmesini veya bu bilgilere kullanılamayacak şekilde hasar verilmesini önlemek ve bu varlık türünü korumaktır (Bilgi Teknolojileri ve İletişim Kurumu, 2018).

Çevrimiçi Güvenlik: Bir kişinin fiziksel ve psikolojik güvenliğinin yanı sıra itibar, kimlik ve çevrimiçi mülkiyeti, donanım, yazılım, bilgi ve fikri mülkiyet de dahil olmak üzere mülkün korunmasıdır (Hartikainen vd., 2019).

Çevrimiçi Öğrenme: Öğrenme materyallerine erişmek, içerik, öğretim elemanı ve öğrenciyle etkileşime geçmek, eğitim sürecini desteklemek için internet teknolojilerinin kullanıldığı yaklaşımdır (Ally, 2004).

Bölüm 2.
Araştırmanın Kuramsal Temeli ve İlgili Araştırmalar

Bu bölümde araştırmanın kuramsal temeline ve bu konuya yönelik alanyazında yer alan ilgili araştırmalara yer verilmiştir.

Sanal ortamlarda bilgi güvenliğine yönelik olarak geliştirilmiş bir çevrimiçi ortamda yürütülen eğitimlerin, ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerine etkisinin incelendiği bu araştırma sürecinde birtakım temel kavramlar yol gösterici olacaktır. Bu bağlamda bilgi güvenliği ve çevrimiçi öğrenme gibi bazı kavramların incelenmesinin önemli olduğu düşünülmektedir.

Bilgi Güvenliği

Bilgi teknolojisi ile ilgili güvenlik riskleri, giderek daha da önemli hale gelen bir konu olmuştur. Bilgi güvenliği, “Bir varlık türü olarak kabul edilen bilgiye başkaları tarafından izinsiz ya da yetkisiz bir şekilde erişilmesini,bu bilginin kullanılmasını, değiştirilmesini, herkese açık olarak paylaşılmasını, yok edilmesini, başkalarına verilmesini veya bu bilgilere kullanılamayacak şekilde hasar verilmesini önlemek ve bu varlık türünü korumak” şeklinde tanımlanmıştır (Bilgi Teknolojileri ve İletişim Kurumu, 2018). Bilgi güvenliğinde “gizlilik”, “bütünlük” ve “erişilebilirlik” unsurlarının öneminden bahsedilmektedir. Bu doğrultuda gizlilik; bilginin yetkisiz kişilerin eline geçmemesi ve yetkisiz erişime karşı korunması; bütünlük, bilginin yetkisiz kişiler tarafından değiştirilmemesi; erişilebilirlik ise bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olması şeklinde tanımlanmıştır (Bilgi Teknolojileri ve İletişim Kurumu, 2018).

Bilgi ve iletişim teknolojileri, kurumların ve bireylerin yüksek verimlilik seviyelerini sürdürmeleri için temel hale gelmiştir. Bu teknolojilerin benimsenmesi, bir dizi yeni güvenlik açığı, dolayısıyla kişisel ve örgütsel verilerin gizliliği ve bütünlüğüne yönelik yeni tehditleri beraberinde getirmiştir (Parsons vd., 2017). Bilgisayar kullanıcılarının tesadüfi ve bilinçsiz davranışları, bilgi güvenliği ihlallerinin en sık nedeni olarak kabul edilmiştir (Parsons vd., 2015). Önceki araştırmalar, çalışanların bilgi güvenliği farkındalığının; bilgi güvenliği ihlalleriyle ilgili riskleri azaltmada hayati derecede önemli olduğunu göstermiştir (Arachchilage & Love, 2014; Safa vd., 2016).

Bu çalışmada ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmeleri incelendiğinden, alanyazında bilgi güvenliğinin ölçümüne yönelik gerçekleştirilmiş çalışmaların incelenmesinde yarar olduğu düşünülmektedir Alanyazın incelendiğinde bilgi güvenliğinin ölçümüne yönelik anketlere sıklıkla başvurulduğu belirlenmiştir. Örneğin, Mylonas vd. (2013) ve Clarke vd. (2016) akıllı telefon kullanımına yönelik kullanıcıların güvenlik bilincini anket aracılığıyla incelemiştir. Benzer şekilde Stanton vd. (2005) şifre ile ilgili davranışlara yönelik bir anket uygulamıştır. Mylonas vd.'nin (2013) Google Play ve Apple Store gibi ortamlardan uygulamalar indiren akıllı telefon kullanıcılarının güvenlik farkındalığını belirleyebilmek amacıyla uyguladıkları anket sonuçlarına göre, kullanıcıların çoğunluğunun uygulama seçiminde ve kurulumu esnasında herhangi bir güvenlik denetimini etkin kılmadıkları belirlenmiştir. Yapılan anket analizi ile çoğunluğun akıllı telefon uygulamalarını uygulama havuzundan indirmenin risksiz olduğuna inandığı sonucuna ulaşılmıştır. Ceran ve Karataş (2021) da yapmış oldukları bir çalışmada insanları olası güvenlik ihlallerine yönelik bilgilendirmek amaçlı bilgi güvenliği konusunda çevrimiçi bir öğrenme sistemi geliştirmeyi amaçlamışlardır. Bu amaç doğrultusunda gerçekleştirdikleri bilgi güvenliğine yönelik alanyazın taraması sonucunda; lisanslı yazılım ve güvenli internet kullanımı, güvenli e-posta kullanımı, güvenli parola politikası, güvenlik yazılımı ve kişisel bilgi paylaşımı konularının kullanıcılara anlatılması gerektiğine karar verilmiştir. Çalışma kapsamında, harcanan emek ve bütçeye rağmen bilgi güvenliğine yönelik tehditlerin azalmadığı, kullanıcıların veya kurumsal sistemlerin maruz kaldığı tehditlerin önlenmesinde yetersiz kalındığı şeklinde belirtilmiştir. Bu bağlamda, 10 yaşındaki bir çocuktan 80 yaşındaki bireye kadar herkesin bilgi güvenliğinin öneminin farkında olması ve kendilerini tehditlerden korunmak için belirli önlemler alabilmesinin gerekliliği vurgulanmıştır.

Stanton vd. (2005) yapmış oldukları bir çalışmada; kullanıcı güvenliği ile ilgili davranışlar hakkında bilgisi olan 110 kişiyle görüşme gerçekleştirmiş, 49 bilişim teknolojisi uzmanı ile bir davranış değerlendirme çalışması yapmış, şifre ile ilgili davranışlarına yönelik 1167 bireye anket uygulamıştır. Anket sonuçları, kullanıcı güvenliği ile ilgili altı davranış kategorisinin iki boyutta derlendiğini göstermiştir. Bu sonuçlara göre, anketin birinci boyutu davranışı uygulamak için gereken teknik bilgi seviyesini belirlerken, ikinci boyutu davranışın niyetini (kötü niyetli, tarafsız ve

yardımsever niyetler) belirlemiştir. Yine anket sonuçları, kötü niyetli olmayan ve düşük teknik bilgi davranışlarına sahip bireylerin şifre belirleme ve paylaşma ile ilgili olarak genel anlamda zayıf olduğunu ortaya koymuştur. Ayrıca, bahsedilen çalışmada iyi şifre belirlemenin ve güvenli kullanımının eğitim, farkındalık, izleme ve motivasyonla ilgili olduğuna dair kanıtlar elde edilmiştir.

Bilgi güvenliği genel olarak bilgilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasına odaklanırken; bilgi güvenliği bilinci veya farkındalığı, etkili bir bilgi güvenliği ortamında güvenlik açısından olumlu davranış oluşturulmasıyla ilgilenir (Kruger & Kearney, 2006). Bilgi güvenliği bilinci, risklerin sürekli değişmesi nedeniyle daha da zorlaşan dinamik bir süreçtir. Sonuç olarak, herhangi bir farkındalık eğitiminin, risk profillerindeki değişiklikleri takip edebilmek için sürekli olarak ölçülmesi ve yönetilmesi gerekir. Kullanıcıların bilgilerini güncel tutmak için, herhangi bir farkındalık eğitimi devam etmeli ve kurum kültürünün ayrılmaz bir parçası olmalıdır. Farkındalıkta başarının anahtarının, sunulan mesajları ilgili ve tutarlı tutmak olduğu vurgulanmaktadır (Kruger & Kearney).

Bilgi güvenliği, siber güvenlik ve veri güvenliği kavramları alanyazında sıklıkla birbirlerinin yerine kullanılabilmektedir. Geleneksel olarak bilgi güvenliği olarak bilinen siber güvenlik, hızla büyüyen ve yüksek öğrenim için artan talep ve fırsatların olduğu önemli bir alandır (Wang, 2017). Siber güvenlik, ABD İç Güvenlik Bakanlığı (The U.S. Department of Homeland Security) altında NICCS (Ulusal Siber Güvenlik Kariyer ve Çalışmaları Girişimi) tarafından "Bilgi ve iletişim sistemlerinin ve burada yer alan bilgilerin korunduğu etkinlik veya süreç, ya da yetkisiz kullanıma veya değiştirmeye veya istismara karşı savunma yeteneği" olarak tanımlanmıştır" (NICCS, 2017).

Sosyal ağların da yoğun bir biçimde kullanıldığı günümüzde dijital veri güvenliği de önemli bir konu olarak göze çarpmaktadır. İnternet ortamı veri güvenliğine yönelik birtakım tehditler barındırmaktadır. E-posta, internet bankacılığı, çevrimiçi alışveriş, virüsler, sosyal ağlarda paylaşılan içerikler dijital veri güvenliğine yönelik tehditler kapsamında düşünülebilir. İnternet ortamındaki tehditlerin farkında olmak ve bireysel önlemler almak mümkündür. Örneğin, güvenlik yazılımlarının güncel tutulması, lisanslı yazılımların kullanılması, güvenli parola tekniklerinin kullanılması, güvenli olmayan e-postalara yönelik dikkatli olunması, sosyal paylaşım

ağlarında kişisel bilgilerin paylaşılmaması, elektronik bankacılık ve çevrimiçi alışverişte bilgilerin kaydedilmemesi alınabilecek bireysel önemler arasındadır.

Kişilerin konu olduğu bilgiler, “isme bağlı veriler” veya “bireysel veriler” şeklinde ifade edilmektedir (Kılınç, 2012). Çeşitli kamu kuruluşları, kâr amaçlı kuruluşlar ve sivil toplum kuruluşları çeşitli türden verileri toplamaktadırlar. Veri güvenliği sorunundan hareketle Türkiye’de kişisel verilerin işlenmesinde kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları esasları düzenlemek amacıyla “Kişisel Verileri Koruma Kanunu” yürürlüğe girmiştir (Kişisel Verileri Koruma Kurumu, 2016). İlgili Kanunda; kişisel verilerin işlenmesi, haklar ve yükümlülükler, başvuru, şikâyet ve veri sorumluları sicili, suçlar ve kabahatler, Kişisel Verileri Koruma Kurumu ve Teşkilat gibi başlıklar altında düzenlemeler yapılmıştır. Yine kişilerin mağduriyetlerini önleyebilmek amacıyla bu kanun kapsamında “Kişisel Veri İhlali Bildirimi” sayfası oluşturulmuştur.

Bilgi güvenliği ev kullanıcıları da dâhil olmak üzere hemen her birey için son derece önemli bir alandır. Çalışmaların çoğu, bireylerin örgütsel ortamdaki davranışlarına odaklanırken, bu davranışlar dolaylı olarak ev kullanıcılarının pratikteki davranışlarından etkilenmektedir. Ne yazık ki, örgütsel kullanıcı davranışları çalışmaları, ev kullanıcılarının bilgi güvenliği tehditleriyle nasıl başa çıktıklarının incelenmesinden yoksundur. Hanus ve Wu (2016) yapmış oldukları bir çalışmada bilgi güvenliği bilincinin masaüstü güvenlik davranışı üzerindeki etkisini incelemek için motivasyon kuramını dikkate almıştır. Çalışma bulgularına göre güvenlik bilincinin algılanan ciddiyetinin, müdahale etkinliğini, öz yeterliliğini ve yanıt maliyetini önemli ölçüde etkilediği raporlanmıştır. Hanus ve Wu’ya göre (2016) internetin ve mobil teknolojilerin yaygınlaşması ile ev kullanıcılarının bilgi güvenliği konusundaki bilinç düzeyi güvenli bir küresel topluluk için önemli bir faktördür. Bununla birlikte, masaüstü güvenliği alanı hala modern toplum için önemli bir endişe olmaya devam etmektedir. Bu doğrultuda ev kullanıcıları arasında bilgi güvenliği farkındalığı uygulamaları teşvik edilmelidir. İnternetin hayatımızın her alanına dâhil olduğu, cep telefonlarında pek çok kişisel verinin depolandığı ve sıklıkla sosyal ağlardan faydalanıldığı göz önünde bulundurularak, bireylerin bilgi güvenliği ve dijital veri güvenliği kavramlarına yönelik farkındalık sahibi olmaları önem arz etmektedir. Bu bağlamda, öğrenci, öğretmen ve velilere yönelik bilgi ve veri

güvenliğine yönelik farkındalık eğitimlerinin planlanmasının, internet ortamındaki tehditlere karşı oldukça önemli bir adım olacağı düşünülmektedir.

Alanyazında bazı araştırmalarda bireylerin bilgi güvenliği tavsiyesine ne ölçüde uyduklarının ölçülebilmesi amacıyla ölçme araçlarının geliştirildiği görülmektedir. Geliştirilen ölçme araçlarında, genellikle çalışma ortamındaki bireylerin bilgi güvenliği bilincinin ya da farkındalığının ölçülmesine odaklanılmıştır. Ölçme araçları bilgi güvenliğinin dar bir kapsamına odaklanmış görünmektedir. Örneğin, ölçme araçlarında şifre koruması kullanımı (Stanton, 2005), mobil cihaz koruması kullanımı (Mylonas vd. 2013) veya güvenlikle ilgili belirli programlarla ilgili özellikler ön plana çıkmaktadır (Hadlington & Chivers, 2018). İş temelli bir bağlamda bireylerin bilgi güvenliği bilincini araştıran ölçme araçlarından birisi de Parsons vd. (2017) tarafından geliştirilen "Bilgi Güvenliği Anketinin İnsani Boyutları" isimli ankettir. Parsons vd. (2017) geliştirmiş oldukları araştırma anketi aracılığıyla bilgi güvenliği farkındalığının yaş aralıkları arasında önemli ölçüde farklı olduğunu ve artan farkındalığın, vicdanlılık ve deneyime açıklıkla pozitif ilişkili olduğunu belirlemiştir.

Bilgi güvenliğinin sağlanması ve verilerin korunması işletmeler için temel bir endişe kaynağı olmaya devam etmektedir. Birçok veri ihlali, maddi veya itibar kaybına yol açan kazara, kasıtlı veya kötü niyetli insan faktörlerinden kaynaklanmaya devam etmektedir. Davranışları ve kültürü geliştirmeye yönelik bir yaklaşım, devam eden farkındalık faaliyetlerinin uygulanmasıdır (Ki-Aries & Faily, 2017). Ki-Aries ve Faily, yapmış oldukları çalışmada; kişileri bilgi güvenliği bilinçlendirme tasarımı ve uygulamasına dâhil ederek güvenlikle ilgili insan faktörlerini tanımlamayı hedeflemişlerdir. Bu doğrultuda 90 günlük farkındalık temaları döngüsüyle bir vaka çalışması gerçekleştirmişlerdir. Çalışma bulguları, kişi merkezli bir bilgi güvenliği farkındalık yaklaşımının, işletme içinde uygulanabilmek için gereken zamana ve kaynağa uyum sağlama kapasitesine sahip olduğunu göstermiştir. Yine kişi merkezli bir bilgi güvenliği farkındalık yaklaşımının güvenlik bilinci yoluyla bilgi güvenliği risklerini azaltmaya olumlu bir katkı sunduğunu belirlemişlerdir.

Sosyal medyanın ve diğer ağ teknolojilerinin yaygın kullanımı, çocuklar için çevrimiçi ortamda bazı güvenlik sorunlarını, riskleri ve tehditleri beraberinde getirebilmektedir. Livingstone ve Smith (2014) tehdidi, mevcut bir güvenlik

açığından kasıtlı olarak veya yanlışlıkla yararlanılabilecek ve bireylere zarar verebilecek bir şey olarak tanımlamaktadır. Zararı, nesnel olarak veya öznel öz bildirim yoluyla ölçülmüş olumsuz bir sonuç; riski ise bir tehdide maruz kaldığında oluşabilecek zarar ve sonuçlara dayanan bir hesaplama olarak tanımlamışlardır. Örneğin, çevrimiçi bazı şiddet içerikleriyle veya cinsel içeriklerle karşılaştıklarında çocukların psikolojik zarar görme riski bulunmaktadır (Livingstone & Smith, 2014).

Çocuklara yönelik internet kullanımıyla ilişkili tehditlerin genellikle içerik tehditlerini ve iletişim tehditlerini içerdiği görülmektedir (Hartikainen vd., 2019). İçerik tehditleri, hedeflenen e-postaları, reklamları, şiddet barındıran içeriği ve uyuşturucuyla ilgili içeriği içerirken; iletişim tehditleri siber zorbalık, siber takip ve gizlilik kaybını içermektedir (Magkos vd., 2014). Boyd ve Hargittai (2013) bu kategorileştirmeyi, yasadışı dosya paylaşımı veya başkalarına zorbalık gibi çocuğun da dâhil olduğu davranış tehditlerini içerecek şekilde genişletmiştir. Magkos vd. özellikle bilgisayarlar ve internet kullanımı ile ilgili tehditleri, kötü amaçlı yazılım, kimlik avı, veri hırsızlığı, veri kaybı, şifre çalma, şifre kırma ve internet bağımlılığı gibi bilgi güvenliği tehditlerini içerecek şekilde genişletmiştir.

Bilgi güvenliğine yönelik bir alanyazın taraması yapıldığında çalışmaların genellikle 15 yaş üzeri, hatta yetişkin bireylere yönelik gerçekleştirildiği görülmektedir (Hanus & Wu, 2016; Mylonas vd., 2013; Stanton vd, 2005). Bilgi güvenliği kavramı özellikle çalışan bireyler için önem arz etse de bu kavramın okul çağındaki çocuklar açısından da önemli olduğu düşünülebilir. Bovina vd. (2014) de bilgi güvenliği kavramının çocuklar açısından anlamını araştıran bir çalışma gerçekleştirmişlerdir. Çalışmada, 19-44 yaş aralığında farklı sosyal gruplardan bireylerle görüşme gerçekleştirilmiş; elde edilen veriler içerik analizi ile çözümlenmiştir. İçerik analizi sonuçları doğrultusunda; bilgiye erişim; internet; sansür; kontrol; bilgi filtreleme; ebeveyn kontrolü ve yasaklar kavramlarının sık kullanıldığı tespit edilmiştir. Çalışma kapsamında elde edilen veriler temalara ayrılmıştır. Bu temalar; güvenliği sağlamanın yolları (kısıtlama, sansür, kontrol, bilgi filtreleme, yasak, koruma, çocuklar için kanallar vb.), geleneksel ve yeni medya (televizyon, internet, sosyal ağ grupları, sohbetler, forumlar vb.), tehditler (saldırganlık, şiddet, uyuşturucu, Nazizm, aşırılık, pornografi vb.), bilgi güvenliği, ebeveynlerin veya öğretmenlerin sorumluluğu (ebeveynlerle iletişim, aile, ebeveyn kontrolü, ebeveynlerin veya öğretmenlerin İnternet kullanımına yardımı vb.),

yasalar-haklar, kişisel verilerin korunması, çocuk bilgilerinin korunması, çocukların bilgi güvenliği ile ilgili eğitim (önleyici sloganlar, çocukların bilgi güvenliği ile ilgili eğitim, ebeveynler için dersler vb.) olarak belirlenmiştir. Çalışmada da görüldüğü üzere bilgi güvenliği kavramı, çocuklar açısından pek çok kavramla bağdaştırılabilmektedir. Alanyazında ise, bilgi güvenliğinin daha geniş bir alanı kapsadığı, bu doğrultuda siber güvenlik, veri güvenliği, çevrimiçi güvenlik kavramlarının kapsam içerisine girdiği görülmektedir.

Çevrimiçi güvenlik, bir kişinin fiziksel ve psikolojik güvenliğinin yanı sıra itibar, kimlik ve çevrimiçi mülkiyeti, donanım, yazılım, bilgi ve fikri mülkiyet de dahil olmak üzere mülkün korunması olarak tanımlanmaktadır (Hartikainen vd., 2019). Alanyazında ebeveynler ve akranları genellikle çocukların çevrimiçi güvenliğinde önemli aktörler olarak görülmektedir (Hasebrink vd., 2011). Okullarda dijital teknolojilerin kullanımı arttıkça, öğretmenler de çocukları korurken interneti güvenli kullanımlarını nasıl teşvik edecekleri sorusuyla karşı karşıyadır (Ahn vd., 2011). Bununla birlikte, çocukların çevrimiçi güvenliği başkalarının eylemlerine bağlı bir şey olarak görülmesinin yanı sıra, çevrimiçi güvenlik çocukların bağımsızlıkları ve gelişimsel süreçleri ile etkinleşen bir eylem olarak da görülebilir (Hartikainen vd., 2019; Wisniewski vd., 2014). Çocukların çevrimiçi güvenliğine aracılık etmek- ebeveyn, öğretmen, endüstri, politika, okullar, farklı yetkililer ve ilgili alanlarda çalışan araştırmacılar gibi- ekip çalışması gerektiren bir konudur. Bununla birlikte çocukların da çevrimiçi güvenlik konusunda farkındalıkları ve bilgi düzeyleri önemlidir.

Hartikainen vd. (2019) çocukların çevrimiçi güvenlik eğitimlerini geliştirmeye yönelik çalışmalara dahil edilmeleri gerektiğine inandıklarını belirtmektedir. Bu doğrultuda yapmış oldukları projede, 2014-2017 yılları arasında Finlandiya'daki çocukların çevrimiçi güvenliği hakkında veri toplamış ve analiz etmişlerdir. Çocukların kendilerine yönelik çevrimiçi güvenlik eğitimi ile nasıl etkileşime girdiklerini ve çevrimiçi güvenlik eğitimini nasıl algıladıklarını anlamak amacıyla, çocuklara yönelik çevrimiçi güvenlik için üç mevcut eğitim paketi ile ilgilenen 11-12 yaş arası çocuklarla atölyeler düzenlenmiş ve gelecekteki eğitim faaliyetleri için beyin fırtınası gerçekleştirilmiştir. Atölye çalışmalarının sonuçlarına dayanarak çocuk-bilgisayar etkileşimi tasarımcılarının ve çevrimiçi güvenlik eğitimi uygulayıcılarının, çocukların kullanımı için çevrimiçi güvenlik konusunda eğitim

paketleri geliştirirken bazı hususlara dikkat etmesi gerektiğini belirtmişlerdir. Bu hususlar; hem çocukların hem de eğitimcilerin hedeflerini ve ilgili değerleri dikkate almak, çocukların kendi medya kültürlerini bütünleştirmek, daha somut tavsiyeler sunmak, olumlu bir tona sahip olmak, hem çocukları hem de öğretmenleri tasarım ve değerlendirmeye dahil etmek şeklinde açıklanmıştır (Hartikainen vd., 2019).

Okullar, internet güvenliği konusunda tüm çocuklara hitap etmek için benzersiz bir konuma sahip durumdadırlar. Yine okullar, ebeveynler tarafından internet güvenliği bilgileri hakkında en güvenilir bilgi kaynağı olarak kabul edilmektedirler. Öğretmenler ve diğer eğitimcilerin, dijital beceriler ve e-güvenlik eğitimi için önemli sorumluluk taşıdıkları ve bu rolü yerine getirmek için desteklenmeleri gerektiği belirtilmektedir (Livingstone vd., 2011). Livingstone vd.'ne göre eğitim sistemiyle ilgili eylemler şunları içermelidir:

1) Okulların internetin yaşa uygun eğitim ve tavsiye sağlayan kullanıcıları olarak daha küçük çocuklara ulaşmanın yeni yollarını geliştirmesi gerekmektedir. Öğretmen eğitiminin, daha küçük çocukları destekleyecek becerilerle donatılması önemlidir.

2) Okullar, yeterli becerilere sahip olunmasını sağlamak için okul dışında internet erişimi olmayanları da dâhil etmeyi amaçlayan özel programlar sağlamalıdır.

3) Pek çok çocuk, çevrimiçi güvenlik uygulamalarıyla ilgili temel becerilere sahip olsa da özellikle kapsamlı farkındalık artırma kampanyalarının odak noktası olan gizlilik ortamlarıyla ilgili becerilere yönelik boşluklar bulunmaktadır. Tüm çocukların asgari bir temel standarda ulaşmasını sağlamak için hem internet güvenliği becerilerini hem de internet kullanımının daha yaratıcı yönlerini öğrenmelerini içerecek şekilde, gençlere yönelik dijital beceri eğitiminin sürekli olarak vurgulanması gerekmektedir.

4) Eğitim, çocukların çevrimiçi içerik ve davranışları kendi kendilerine yönetmelerine özellikle dikkat etmeli ve çevrimiçi içerik yayınlamanın yararlarının ve risklerinin daha eleştirel bir şekilde farkına varmalarını sağlamalıdır.

Zilka (2017) çevrimiçi gizlilik, siber zorbalık, şiddet barındıran içeriğe maruz kalma, dışlanma ve nefreti körükleyen içeriğe maruz kalma, yabancılarla çevrimiçi iletişim ve kaba dil kullanımı gibi unsurları içeren güvenliğin önemli bir sorun haline geldiğini belirtmektedir. Yapmış olduğu çalışmada, çocukların ve gençlerin e-güvenlik ve potansiyel çevrimiçi tehlikeler konusundaki farkındalık düzeylerini değerlendirmiştir. Çalışmasında e-güvenlik ifadesini, interneti çocuklar ve gençler tarafından kullanmanın potansiyel tehlikeleri hakkındaki farkındalık olarak tanımlamıştır. E-güvenlik bilinci şiddet barındıran içeriğe maruz kalma, kaçınma veya yapma derecesi, çevrimiçi yabancılarla iletişim kurma, çevrimiçi tehlikelerle başa çıkmalarına yardımcı olacak araçlara ihtiyaç duydukları derece ve kendilerini "ihtiyatlı internet kullanıcıları" olarak tanımladıkları derece ile ilişkilendirilmiştir.

Çevrimiçi güvenlik teması bağlamında dikkat çeken konulardan birisi de çevrimiçi mahremiyettir. Sosyal medya araçlarının oldukça küçük yaş gruplarınca kullanıldığını düşünerek; öğrencilerin çevrimiçi mahremiyet konusunda farkındalık kazanmalarının öneminden bahsetmek mümkündür. Özellikle ortaokul ve lise düzeyinde mahremiyet becerilerine güçlü bir vurgu yapan birçok eğitim programı geliştirilmiştir (Common Sense Media, 2021; International Computer Science Institute, 2021; Office of the Privacy Commissioner of Canada, 2019; Raynes-Goldie & Allen, 2014). Ancak, Finkelhor vd. (2021) son derece önemli olan bilgi ve mahremiyet kavramlarının veya diğer koruma becerilerinin çocuklukta edinilmesine yönelik etkili bir eğitimin tasarlanması hakkında çok az bilgiye sahip olunduğunu vurgulamaktadır. Sosyal medya platformlarında bilgi saklama konusunda gençlerin yetişkinlerle aynı endişeleri taşımayabileceğine dair bulgulara rastlanmaktadır. Örneğin Livingstone vd. (2014) yapmış oldukları çalışmada; Avrupa'da yaşayan 9-16 yaş aralığındaki 10.000 çocuğa yönelik açık uçlu bir anket sorusunda, çocukları ilgilendiren internet risklerini araştırmışlardır. Araştırma sonuçları pornografinin çocukların %22'si; siber zorbalığın %19'u; şiddet içeriğinin çocukların %18'i tarafından endişe sebebi olarak görüldüğünü göstermiştir.

Çocukları çevrimiçi mahremiyetin yönetimi konusunda eğiten bir oyunun tasarım sürecinin ve sonuçlarının araştırıldığı bir çalışmada (Raynes-Goldie & Allen, 2014) çocukların bazı yetişkin algılarına kıyasla oldukça karmaşık mahremiyet anlayışlarına sahip oldukları ve onlardan kişisel veri toplamaya çalışan ticari kuruluşların oluşturduğu risklerin farkında oldukları belirtilmiştir. Yine; internetin ve

sosyal medyanın günlük yaşamda artan kullanımının, özellikle çocuklarla ilgili olarak, çevrimiçi güvenlik ve mahremiyet konusunda artan endişelere sebep olduğu, bu tür endişelerin öncelikle yetişkinler tarafından ifade edildiği ve buna göre pek çok girişimin, çocukların teknoloji kullanımlarına ilişkin yetişkinlerin algılarına dayandığı vurgulanmıştır.

Gençlere yönelik internet güvenliği eğitim programlarının incelendiği bir çalışma kapsamında yapılan alanyazın taraması sonuçları; internet güvenliğini, hâlihazırda ilgili çevrimdışı zararları ele alan (örneğin genel zorbalık, flört istismarı veya cinsel istismarı önlemeye odaklanan) programlar gibi halihazırda iyi yapılandırılmış ve kanıta dayalı eğitimlere entegre etmenin büyük avantajlarının olacağını göstermektedir. Bu avantajların dört faktörden kaynaklanabileceği açıklanmıştır:

1) Çevrimiçi zararlar ve benzer çevrimdışı zararlar arasında önemli benzerliklerin olması,
2) Çevrimdışı zararların görünürde daha yaygın olması,
3) Hem çevrimiçi hem de çevrimdışı zararların arkasında aynı risk faktörlerinin yattığına dair kanıtlar olması,
4) Orijinal olarak çevrimdışı zararlar etrafında geliştirilen daha uzun süreli eğitimler için önemli ölçüde kanıtlar olması (Finkelhor vd., 2020).

Çevrimiçi tehlikeler hakkında yıllardır yapılan uyarılara rağmen, çok sayıda kişi hala çevrimiçi güvenlik standartlarına uymamaktadır. Her internet kullanıcısı genel ağın bütünlüğünü korumada bir rol oynamakta; bireyler istemeden de olsa suç güçlerinin hesaplarına veya makinelerine erişmesine izin vererek genel güvenliği tehlikeye atabilmektedirler (Shillair vd., 2015). Çevrimiçi güvenliğin sağlanmasında bireysel ev bilgisayarı kullanıcılarının rolünün araştırıldığı bir başka çalışmada; geniş bir demografik ve sosyoekonomik geçmişe sahip 594 ev bilgisayarı kullanıcısından bir anket aracılığıyla veri toplanmıştır. Elde edilen sonuçlar, ev bilgisayarı kullanıcılarının güvenlikle ilgili davranış sergileme niyetinin bilişsel, sosyal ve psikolojik bileşenlerin bir kombinasyonundan etkilendiğini göstermiştir (Anderson & Agarwal, 2010).

“Bilgi güvenliği” teması bağlamında alanyazına yönelik genel bir değerlendirme yapmak gerekirse; sanal ortamlarda bilgi güvenliği konusunda

kullanıcı davranışlarının ve bilincinin kilit rol oynadığı; çocukların çevrimiçi ortamlardaki risk ve tehditler hakkında bilgi sahibi olmalarının önemli olduğunu söylemek mümkündür.

Çevrimiçi Öğrenme ve Uzaktan Eğitim

Çevrimiçi öğrenme, e-öğrenme, çevrimiçi eğitim ve uzaktan eğitim kavramları zaman zaman aynı anlamda kullanılabilmektedir. Bu bağlamda bu kavramlara yönelik açıklama yapılmasında yarar olduğu düşünülmektedir.

Uzaktan eğitim, genellikle coğrafi olarak uzak olanlara öğrenmeye erişim sağlama çabasını anlatmaktadır (Moore vd., 2011). Bilgisayarlar eğitime dâhil olmaya başladıkça, uzaktan eğitime yönelik “hem basılı hem de elektronik medyayı kullanarak öğretim materyallerinin kullanımı” tanımı gündeme gelmiştir (Moore, 1990). Tüm tanımlarda bulunan ortak noktaların, iki taraf (bir öğrenci ve bir eğitmen) arasında bir tür etkileşimin gerçekleşmesi, farklı zamanlarda ve / veya yerlerde yapılması ve çeşitli öğretim materyallerinin kullanması olduğu söylenebilir (Moore vd., 2011).

Yetişkinlere yönelik uzaktan eğitim programlarında olduğu gibi, K-12 düzeyindeki uzaktan eğitim, geleneksel "evde çalışma" ya da metin tabanlı yazışma programlarından, teknoloji aracılığıyla öğretimin tüm potansiyelini kullanan programlara kadar pek çok uygulamayı içermektedir (Rice, 2006). Bilgisayarlar eğitimin her alanında sıklıkla kullanılmakta ve öğrenciler ders ortamlarına bilgisayar, tablet ve akıllı telefonlar gibi çeşitli cihazlar aracılığıyla erişebilmektedirler. Yine; bu cihazların ürettiği veriler, etkinlik akışları olarak öğrencilere iletilebilmektedir. Etkinlik akışı; öğrencileri kursun mevcut durumu hakkında bilgilendiren, zamana dayalı sistem etkinliklerinin (belge yüklemeleri, öğrenci yorumları ve tartışmaları, önemli olayların bildirimleri gibi) bir listesidir. Facebook ve Twitter gibi sosyal ağların kullanımı, kullanıcılarına en son haber güncellemelerini, durum değişikliklerini ve paylaşılan hikâyeleri bildirmek için etkinlik akışlarının kullanımını teşvik etmiştir. Bu sosyal medya türü etkinlik akışları kavramı, öğrenci için oldukça faydalı olabilecek toplu etkinliklerin bildirimini içerecek şekilde eğitime yansıtılabilir (Gunawardena, 2017). Eğitim bağlamında, kişiselleştirilmiş etkinlik akışları sürekli olarak yayınlandığı için öğrenci motivasyonunu (Wankel & Blessinger, 2012) artırma potansiyeline sahiptirler. Verilerin eğitimdeki rolü, yalnızca dijital çağın öncesindeki

içeriği (ders kitapları ve anketler) dijital çağa aktarmak değil, aynı zamanda daha nitelikli zengin veriler sunmaktır (Gunawardena, 2017). Geçmişten farklı olarak, öğrencilerin kavramları anlama durumunu ölçmek için öğrenme etkinlikleri tasarlayarak veri üretmek kolaylaşmıştır. Örneğin, vurgulanan pasajlar ve öğrenci yorumları, eğitmenleri belirli bir kavramın toplu veya bireysel olarak anlaşılıp anlaşılmadığı konusunda bilgilendirebilmektedir.

Bu çalışma kapsamında ortaokul öğrencileri sanal ortamda bilgi güvenliğine ilişkin öğrenmelerine yönelik geliştirilmiş bir çevrimiçi ortamda eğitimlere katılmışlardır. Bu bağlamda uzaktan eğitimdeki etkileşim unsurlarının incelenmesinde yarar olduğu düşünülmektedir. Moore (1997) uzaktan eğitimin, öğretmen ile öğrenen arasında, öğretmenin öğrenenden ayrılması gibi özel bir niteliğe sahip bir ortamda gerçekleştiğine dikkat çekmektedir. Yine uzaktan eğitimde, öğrenci ve öğretmenlerin ayrılmasının hem öğretmeyi hem de öğrenmeyi derinden etkileyeceği ve eğitmenin girdileri ile öğrencinin girdileri arasında potansiyel bir yanlış anlama alanı olacağı vurgulanmaktadır. Bununla birlikte, uzaktan eğitimde, öğretmen ve öğrencinin ayrılması, kullandıkları özel öğretme-öğrenme stratejileri ve tekniklerinin bu eğitim uygulamaları ailesinin ayırt edici özellikleri olarak tanımlanabilmesi için yeterince önemlidir. Kullanılan öğretme-öğrenme stratejileri ve teknikleri ile öğretmenlerin ve öğrencilerin davranışlarında da çok büyük farklılıklar olduğu bu durumun ise uzaktan eğitim programları içinde farklı derecelerde iletişimsel mesafe oluşturduğu şeklinde yorumlanabileceği vurgulanmaktadır. Bu sorunlar bağlamında, uzaktan eğitime yönelik etkileşimsel uzaklık kuramı geliştirilmiştir. Bir eğitim programında etkileşimsel uzaklığın kapsamı, teknolojik veya iletişim değişkenleri değil; öğretme ve öğrenme etkileşimindeki değişkenlerdir. Bu değişken kümeleri; diyalog, program yapısı ve öğrenen özerkliği şeklinde adlandırılmıştır (Moore):

1) Diyalog: “Diyalog” terimi, olumlu niteliklere sahip bir etkileşimi veya bir dizi etkileşimi tanımlamak için kullanmaktadır. Eğitimsel bir ilişkide diyaloğun yönü, öğrencinin daha iyi anlaşılmasına yöneliktir. Diyaloğun kapsamı ve doğası; kursun tasarımından sorumlu olan bireyin veya grubun eğitim felsefesi, öğretmen ve öğrencinin kişilikleri, kursun konusu ve çevresel faktörler tarafından belirlenir. Çevresel faktörlerin en önemlilerinden biri iletişim ortamıdır. Uzaktan eğitim alanı geliştikçe iletişim medyasının yanı sıra;

özellikle derslerin tasarımı, eğitmenlerin seçimi, yetiştirilmesi ve öğrencilerin öğrenme stilleri gibi değişkenlere daha fazla önem verilmesi gerekmektedir.

2) Program Yapısı: Etkileşimsel uzaklığı belirleyen ikinci değişken grubu, ders tasarımındaki ögeler veya çeşitli iletişim ortamları aracılığıyla iletilebilmesi için öğretim programının yapılandırılma biçimleridir. Yapı, programın eğitim hedeflerinin, öğretim stratejilerinin ve değerlendirme yöntemlerinin katılığını veya esnekliğini ifade eder. Bir eğitim programının her bir öğrencinin bireysel ihtiyaçlarını ne ölçüde karşılayabileceğini veya bunlara ne ölçüde yanıt verebileceğini tanımlar. Başarılı uzaktan öğretim; kuruma, bireysel eğitmenin öğretmen ve öğrenci arasındaki diyaloğu için uygun fırsatları sağlamasına ayrıca uygun şekilde yapılandırılmış öğrenme materyallerine bağlıdır. Pratikte program yapısı; içeriğe, öğretim düzeyine ve öğrenen özelliklerine, özellikle de öğrencinin uygulayabileceği optimum özerkliğe göre değişmektedir. Öğrenci özelliklerinin anlaşılmasının yanı sıra zaman ve çabanın, herhangi bir programda ihtiyaç duyulan yapının kapsamını belirlemeye ve uygun şekilde yapılandırılmış sunumlar ve etkileşimler tasarlamaya ayrılması gerektiği belirtilmektedir. Uzaktan eğitimde; öğretim neredeyse hiçbir zaman bireysel bir eylem değildir, tasarım ekipleri ve dağıtım ağlarındaki bir dizi uzmanın uzmanlığını bir araya getiren işbirlikçi bir süreçtir. Her bir uzaktan eğitim programında yapılandırılması gereken süreçlerden bazıları şu şekilde açıklanmıştır:

    a. Sunum: Pek çok programda bilgi sunumları, beceri gösterimleri veya tutum ve değer modelleri yer almaktadır.

    b. Öğrencinin motivasyonunun desteklenmesi: Bir müfredat, öğretilecek bir içerik programı planlandıktan sonra, ders tasarımcıları ve eğitmenler, öğrencinin öğretilecek olanlara ilgisini teşvik etmeli, öğrenciyi öğrenmeye motive etmeli, öğrenmeyi geliştirmeli ve sürdürmelidir.

    c. Analizin ve eleştirinin teşvik edilmesi: Analizin ve eleştirinin teşvik edilmesi, öğrencilerin yükseköğretimde geliştirmeleri beklenen üst düzey bilişsel becerilerdir. Bu tür beceri ve tutumların gelişimini

uzaktan yapılandırmak özellikle zordur. Öğrenciye kayıtlı içerikleri analiz etmesi için yardım edilmelidir.

d. Tavsiye verilmesi: Eğitim programı, öğrenme materyallerinin kullanımı hakkında rehberlik sağlamalı ve çalışma becerilerini geliştirme ve çalışma problemleriyle uğraşma konusunda yardıma ihtiyaç duyan bireyler için bir tür referans sağlamalıdır.

e. Uygulama, test ve değerlendirmelerin düzenlenmesi: Öğrencilere, gösterilen becerilerin uygulanması için veya sunulan bilgi ve öğrenilenleri uygulaması için fırsat verilmelidir.

f. Öğrencinin bilgi oluşturma süreci için düzenleme yapılması: Öğrencilere bilgi oluşturma sürecinde öğretmenlerle yeterli diyaloga girme fırsatı sağlanmalıdır.

3) Öğrenen Özerkliği: Öğrenen özerkliği; öğretme/öğrenme ilişkisinde öğrenme programının amaçlarını, öğrenme deneyimlerini ve değerlendirme kararlarını öğretmenden ziyade öğrencinin belirleme derecesidir. Uzaktan eğitim programları, öğretmenin veya öğrencinin ana öğretme-öğrenme süreçlerini ne ölçüde kontrol ettiğini görmek için incelenebilir ve her programın izin verdiği öğrenci özerkliği derecesine göre sınıflandırılabilir. Özerk öğrenenler olarak ileri düzeyde yetkinliğe sahip öğrencilerin daha az diyalog içeren programlarla oldukça rahat göründükleri; daha bağımlı öğrencilerin ise daha fazla diyalog içeren programları tercih ettikleri belirtilmiştir (Moore,1997).

Alanyazında uzaktan eğitim kavramıyla zaman zaman aynı anlamda kullanılmakta olan “çevrimiçi öğrenme” kavramının da incelenmesinde yarar olduğu düşünülmektedir. Çevrimiçi öğrenme uzaktan eğitimin alt bileşeni olarak ele alınmaktadır (Anderson, 2008). Posta hizmeti yoluyla temel yazışmalardan internet aracılığıyla kullanılabilen çok çeşitli araçlara kadar, yıllar boyunca yeni iletişim biçimleri benimsenmiştir. Böyle bir form olan çevrimiçi öğrenmenin 1980'lerde başlayan bir erişim geçmişine sahip olduğu bilinmektedir (Harasim, 2000). Farklı öğrenme ortamlarının tasarımı; öğrenme hedefine, hedef kitleye, erişime (fiziksel, sanal ve / veya her ikisi) ve içerik türüne bağlı olabilmektedir. Moore vd. (2011) öğrenme ortamının nasıl kullanıldığına ve öğrenme çıktılarındaki farklılıkları ayırt eden araç ve tekniklerin etkilerini bilmenin önemine vurgu yapmaktadır.

Çevrimiçi öğrenme için yaygın olarak kullanılan terimler arasında e-öğrenme, dağıtılmış öğrenme, ağa bağlı öğrenme, tele-öğrenme, sanal öğrenme, bilgisayar destekli öğrenme, web tabanlı öğrenme ve uzaktan öğrenme yer alır. Khan (1997) çevrimiçi eğitimi, Web'i ortam olarak kullanarak uzak bir kitleye eğitim vermek için yenilikçi bir yaklaşım olarak tanımlamaktadır. Ally (2008) ise; çevrimiçi öğrenmeyi, "öğrenme materyallerine erişmek için internet kullanımı; içerik, eğitmen ve diğer öğrencilerle etkileşimde bulunmak; öğrenme süreci boyunca, bilgi edinmek, kişisel anlam oluşturmak ve öğrenme deneyiminden büyümek için destek almak" şeklinde tanımlamaktadır. Çevrimiçi öğrenmenin, katılımcıların zaman ve mekânı bağımsızlaştırmasına olanak tanıması, öğrenme materyallerinin de öğrenciyi meşgul edecek ve öğrenmeyi teşvik edecek şekilde tasarlanması gerekmektedir. E-Öğrenme ise öğretim etkinliklerinin elektronik ortamlarda yürütülmesi veya bilgi ve becerilerin elektronik ortamda aktarılması olarak tanımlanmaktadır (Gülbahar, 2019). E-öğrenmeye yönelik bir başka tanım ise şu şekildedir:

> *"E-öğrenme, bilgi ve iletişim teknolojileri yardımı ve internet/intranet gibi yerel ve geniş alan ağları aracılığı ile zaman ve mekândan bağımsız olarak bilgiye erişimi ve çoklu ortam uygulamaları ile etkileşim sağlanarak, öğretim etkinliklerinin elektronik öğrenme ortamlarında yürütülmesidir" (Gülbahar, 2019).*

İnternetin gelişiyle birlikte, dünyanın dört bir yanındaki öğrencilere ulaşma potansiyeli büyük ölçüde artmış ve günümüzün çevrimiçi öğrenimi, birden çok medyada zengin eğitim kaynakları ve eğitmenler ile öğrenciler arasında hem gerçek zamanlı hem de eş zamansız iletişimi destekleme yeteneği sunmuştur. Yükseköğretim kurumları ve kurumsal eğitim, çevrimiçi öğrenimi hızlı bir şekilde benimserken, önceleri K–12 okul sistemleri geride kalsa da bu sektör de e-öğrenmeyi benimseme konusunda hızla ilerlemiştir (Means, 2009). Çevrimiçi öğrenme, içeriğe ve eğitime herhangi bir zamanda, herhangi bir yerden daha esnek erişim sağlama potansiyeli nedeniyle popüler hale gelmiştir. Çoğunlukla çevrimiçi öğrenmenin odak noktaları, geleneksel yüz yüze sunumlara katılamayan veya katılmamayı seçen öğrenciler için öğrenme deneyimlerinin kullanılabilirliğini arttırmak, öğretim içeriğini daha uygun maliyetli bir şekilde bir araya getirmek ve yaymak veya eğitmenlerin karşılaştırılabilir yüz yüze eğitime eşdeğer öğrenme kalitesini korurken daha fazla öğrenciye ulaşabilmesini sağlamak olarak belirtilmiştir (Means vd., 2009).

Farklı çevrimiçi öğrenme modellerini desteklemek için farklı teknoloji uygulamaları kullanılmaktadır. Eş zamanlı etkinlikler, tüm katılımcıların aynı zaman içerisinde çevrimiçi olduğu etkinlikler olarak tanımlanmaktadır. Eş zamanlı etkinlikler iyi bir planlama gerektirmektedirler. Eş zamansız etkinlikler ise katılımcıların aynı anda bir arada olmasını gerektirmeyen etkinlikler olarak tanımlanmaktadır. Eş zamansız etkinliklerde katılım için esnek zaman sağlanması, katılımcıların kendileri için en uygun zamanda etkinliklere katılmasına imkân tanımaktadır (Gülbahar, 2019). Eş zamansız iletişim araçları (örneğin, e-posta, ileti dizisi içeren tartışma panoları, haber grupları) kullanıcıların rahatlıklarına katkıda bulunmalarına olanak sağlamak için kullanılırken, eşzamanlı teknolojiler (örneğin, Web yayını, sohbet odaları, masaüstü ses / video teknolojisi) ders verme ve öğrenci gruplarıyla toplantı yapma gibi yüz yüze öğretim stratejilerini belirlemek için kullanılmaktadır. Daha önceki çevrimiçi programlar, bir modeli veya diğerini uygulama eğilimindeyken, yeni uygulamalar, eş zamanlı ve eş zamansız çevrimiçi etkileşimlerin birden çok biçimini ve ayrıca ara sıra yüz yüze etkileşimleri birleştirme eğilimindedir (Means vd., 2009). Means vd. çevrimiçi öğrenmeyi tanımlayan üç temel bileşeni şu şekilde açıklamıştır:

1) Faaliyetin geleneksel yüz yüze öğretimin yerini alması veya yüz yüze öğretimi geliştirmesi,
2) Öğrenme deneyimi türü (pedagojik yaklaşım),
3) İletişimin birincil olarak eşzamanlı veya eş zamansız olması.

Çevrimiçi ortamlarda yürütülecek eğitimlerin planlanmasında eğitimin etkililiğinin belirlenmesi önemli bir konudur. Örneğin öğrenme çıktıları açısından geleneksel öğretime eşdeğer bir uygulama, öğrenci başarısından ödün vermeden çevrimiçi öğrenmeyi sağlıyorsa başarılı kabul edilebilir. Bir kursun çevrimiçi veya yüz yüze alınmasından bağımsız olarak öğrenci başarısı aynı düzeydeyse, çevrimiçi öğretim, belirli bir coğrafi bölgede çok az öğrencinin bulunduğu ortamlarda uygun maliyetli bir şekilde kullanılabilir (örneğin; kırsal kesim öğrencileri, uzmanlık kurslarındaki öğrenciler). Bunun tersine, yalnızca yüz yüze eğitimdeki öğrenci başarısı ya da öğrenme çıktıları üreten çevrimiçi faaliyetler, zaman ve para kaybı olarak değerlendirilir (Means vd., 2009). Çevrimiçi eğitimde ikinci bir önemli boyut, öğrenenlerin bilgi edinme şeklini kimin (veya neyin) belirlediğine bağlı olan öğrenme deneyimi türüdür. Öğrenme deneyimleri, öğrencinin öğrenme etkinliğinin içeriği ve

doğası üzerinde sahip olduğu kontrol miktarına göre sınıflandırılabilir. Geleneksel didaktik veya açıklayıcı öğrenme deneyimlerinde, içerik öğrenciye bir ders, yazılı materyal veya diğer mekanizmalarla iletilir. Başka bir öğrenme deneyimi kategorisi, öğrenenlerin birbirleriyle ve bir öğretmenle veya diğer bilgi kaynaklarıyla etkileşime girdikçe öğrenme içeriğinin doğasının ortaya çıktığı işbirliğine dayalı veya etkileşimli öğrenme faaliyetini vurgular. Çevrimiçi öğrenme etkinliklerini kategorilere ayırmak için yaygın olarak kullanılan üçüncü bir özellik, faaliyetin gerçek zamanlı olarak fiziksel veya sanal bir yerde veya eş zamansız olarak, öğretim uyaranlarının sunumu arasında bir zaman gecikmesi ile ne derece senkronize olduğudur (Means vd., 2009).

Çevrimiçi öğrenme teknolojileri Açıklayıcı yönerge, aktif öğrenme ve etkileşimli öğrenme olmak üzere üç farklı öğrenme deneyimini destekleyebilir:

1) Açıklayıcı yönerge: Dijital cihazlar bilgi aktarır.
2) Aktif öğrenme: Öğrenci, çevrimiçi alıştırmalar, simülasyonlar, oyunlar veya mikro dünyalar gibi dijital eserlerin sorgulamaya dayalı manipülasyonu yoluyla bilgi oluşturur.
3) Etkileşimli öğrenme: Öğrenci, diğer öğrencilerle sorgulamaya dayalı işbirliğine dayalı etkileşim yoluyla bilgi oluşturur; öğretmenler rehber olarak hareket ederler.

Öğrenmenin sadece okullarla ve örgün eğitimle sınırlı kalamayacağı gerçeğinden hareketle çevrimiçi öğrenmenin birtakım avantajlarından bahsedilmesinde yarar vardır. Ally (2008) çevrimiçi öğrenmenin avantajlarını öğrenciler ve eğitimciler açısından değerlendirmiştir. Ally'ye göre öğrenciler için çevrimiçi öğrenmede konum ve mesafe sorun değildir. Eş zamansız çevrimiçi öğrenmede, öğrenciler çevrimiçi materyallere her zaman erişebilirken, eş zamanlı çevrimiçi öğrenme öğrenciler ve eğitmenler arasında gerçek zamanlı etkileşime izin verir. Öğrenciler interneti güncel ve ilgili öğrenme materyallerine erişmek için kullanabilir ve çalıştıkları alandaki uzmanlarla iletişim kurabilirler. Öğrenciler kendi iş yerlerinde çalışırken çevrimiçi kursları tamamlayabilir ve öğrenmeyi bağlamsallaştırabilirler. Eğitmenler için ise dersler her zaman, her yerde yapılabilir, çevrimiçi materyaller güncellenebilir ve öğrenciler değişiklikleri hemen görebilirler. Öğrenciler İnternet'teki materyallere erişebildiklerinde, eğitmenlerin bunları

ihtiyaçlarına göre uygun bilgilere yönlendirmeleri daha kolaydır. Çevrimiçi öğrenme sistemleri düzgün tasarlanırsa, öğrencilerin ihtiyaçlarını ve mevcut uzmanlık düzeyini belirlemek ve öğrencilerin de seçtikleri öğrenme çıktılarını elde etmeleri için seçebilecekleri uygun materyaller sağlamak amacıyla kullanılabilir.

Çevrimiçi öğrenme kavramının yanı sıra çevrimiçi eğitim kavramına yönelik açıklama yapılmasında yarar vardır. Çevrimiçi eğitim için alanyazında; sanal eğitim, internet tabanlı eğitim, web tabanlı eğitim ve bilgisayar aracılı iletişim yoluyla eğitim gibi birçok terimin kullanıldığı görülmektedir. Web Education Systems (Web-edu) projesi kapsamında Keegan'ın (1988) uzaktan eğitim tanımı temel alınarak çevrimiçi eğitim şu şekilde karakterize edilmiştir (Paulsen, 2002):

1) Yüz yüze eğitimden farklı yanı öğrenci ve öğretmenin ayrılmış olması,
2) Bir eğitim kurumunun kendi kendine çalışma ve özel derslikten ayrı olması,
3) Bazı eğitim içeriğini sunmak veya dağıtmak için bir bilgisayar ağının kullanılması,
4) Öğrencilerin birbirleri, öğretmenler ve personel ile iletişimden yararlanabilmeleri için bilgisayar ağı üzerinden iki yönlü iletişim sağlanması.

Bu çalışma kapsamında sanal ortamlarda bilgi güvenliğine yönelik geliştirilmiş olan bir çevrimiçi ortamda eğitimler yürütüldüğünden, öğrenme kuramlarının incelenmesinde yarar olduğu düşünülmektedir. En uygun öğretim stratejilerini seçmek için, çevrimiçi geliştiriciler farklı öğrenme yaklaşımlarını bilmelidirler. Öğrencileri motive etmek, derin işlemeyi kolaylaştırmak, tüm kişiyi inşa etmek, bireysel farklılıklara hitap etmek, anlamlı öğrenmeyi teşvik etmek, etkileşimi teşvik etmek, ilgili geribildirimi sağlamak, kolaylaştırmak için çeşitli stratejiler seçilmelidir (Ally, 2008). Çevrimiçi öğrenme için, davranışçı öğrenme kuramı, bilişsel öğrenme kuramı, yapılandırmacı öğrenme kuramı ve bağlantıcı öğrenme kuramlarının etkilerinin incelenmesinde yarar olduğu düşünülmektedir.

Davranışçı kuramda; bir uyaranda bir yanıtın niceliksel olarak gözlemlenebilmesi açısından zihin kara bir kutu olarak görülmektedir. Davranışçı öğrenme kuramının çevrimiçi öğrenmeye etkisi şu şekilde düşünülebilir (Ally, 2008):

1) Öğrencilere öğrenmenin açık sonuçları ve hedefleri anlatılmalıdır, böylece öğrenciler kendi beklentileri belirleyebilirler.

2) Öğrencilerin, öğrenme hedeflerine ulaşıp ulaşmadıklarını belirlemek için test edilmeleri gerekir. Çevrimiçi testler veya diğer test ve değerlendirme biçimleri, öğrencinin başarı seviyesini kontrol etmek ve uygun geribildirimi sağlamak için öğrenme-öğretme süreçleriyle kaynaştırılmalıdır.

3) Öğrenmeyi teşvik etmek için öğrenme materyalleri uygun şekilde basitten karmaşığa doğru sıralanmalıdır.

4) Öğrencilere, nasıl çalıştıklarını izleyebilmeleri ve gerektiğinde düzeltici önlemler alabilmeleri için geri bildirim sağlanmalıdır.

Bilişsel öğrenme kuramında öğrenme; bellek, düşünme, yansıtma, soyutlama, motivasyon ve metabilişselliği içeren dahili bir süreç olarak görülür. Bilişsel öğrenme kuramının çevrimiçi öğrenmeye etkisi şu şekilde sıralanabilir (Ally, 2008):

1) Kullanılan stratejiler, öğrencilerin bilgiyi çalışma belleğine aktarılabilmesi için algılamasına izin vermelidir.

2) Kullanılan stratejiler, öğrencilerin yeni bilgileri anlamasına yardımcı olmak için mevcut bilgileri uzun süreli bellekten almalarına izin vermelidir.

3) Çalışma belleğinde işlem sırasında aşırı yüklenmeyi önlemek için bilgiler parçalara ayrılarak sunulmalıdır (Miller, 1956). Çalışan bellekte verimli işlemeyi kolaylaştırmak için, çevrimiçi öğrenme materyalleri bir ekranda beş ila dokuz öge sunmalıdır (Miller, 1956).

4) Bilginin uzun süreli belleğe aktarımını daha etkili hale getirmek için, öğrencilerin üst düzey öğrenmeyi teşvik etmelerini, analiz etmelerini, sentezlemelerini ve değerlendirmelerini gerektiren stratejiler kullanılmalıdır.

5) Bireysel farklılıklara ve öğrenme stillerine uyum sağlamak için çevrimiçi eğitime çeşitli öğrenme stratejileri dâhil edilmelidir (Cassidy, 2004).

6) Bilgilerin işlenmesini ve uzun süreli belleğe aktarılmasını kolaylaştırmak için bilgi, farklı modlarda sunulmalıdır.

7) Öğrenciler öğrenmeye motive edilmelidir.

8) Üstbiliş, bir öğrencinin bilişsel yeteneklerinin farkında olma ve bu yetenekleri öğrenmek için kullanma yeteneğidir. Çevrimiçi ortamlarda öğrenirken; öğrendikleri şeyleri yansıtmak, diğer öğrencilerle işbirliği yapmak ve ilerlemelerini kontrol etmek için öğrencilere fırsat verilmelidir.

9) Öğrenme aktarımını kolaylaştıran çevrimiçi stratejiler, farklı ve gerçek yaşam durumlarında uygulamayı teşvik etmek için kullanılmalıdır. Öğrencilere gerçek hayattaki uygulamaları ve bilgileri kullanan ödevleri ve projeleri tamamlama fırsatı verilmelidir (Ally, 2008).

Çevrimiçi öğrenmede motivasyon oldukça önemli bir bileşendir. Keller (1987) öğrenenleri öğrenme sırasında motive etmek için ARCS modelini (Dikkat, İlgi, Güven, Memnuniyet) önermektedir:

a) Dikkat: Dersin başında öğrencilerin dikkati çekilmeli ve bu durum ders boyunca devam ettirilmelidir. Çevrimiçi öğrenme materyalleri, öğrencilerle bağlantı kurmak için öğrenme oturumunun başlangıcında bir etkinlik içermelidir.

b) İlgi: Öğrenciler dersin önemi ve ders almanın onlara nasıl fayda sağlayabileceği hakkında bilgilendirilmelidir. Bu hususta kullanılacak stratejiler, öğrencilerin dersi almaktan nasıl faydalanacaklarını ve öğrendiklerini gerçek hayatta nasıl kullanabileceklerini açıklamayı içerebilir.

c) Güven: Öğrencileri ders beklentileri hakkında bilgilendirmek gibi stratejiler kullanılmalıdır. Basitten karmaşığa veya bilinenden bilinmeyene doğru sıralayarak tasarım yapılmalı ve öğrencilere dersi tamamlamak için farklı stratejiler kullanma fırsatı verilen yetkinlik tabanlı bir yaklaşım kullanılmalıdır. Öğrenciler ders sonuçları hakkında bilgilendirilmeli ve dersi tamamlamak için sürekli teşvik edilmelidir.

d) Memnuniyet: Öğrencilerin performansı hakkında geri bildirimde bulunulmalı ve öğrendiklerini gerçek yaşam durumlarında uygulamalarına izin verilmelidir.

Bu çalışma kapsamında sanal ortamda bilgi güvenliği eğitimine yönelik geliştirilen çevrimiçi ortamın tasarlanma sürecinde öğrenme kuramları ve ARCS modeli dikkate alınmıştır. Herhangi bir öğretim sisteminin amacı öğrenmeyi teşvik etmektir. Bu nedenle, herhangi bir öğrenme materyali geliştirilmeden önce, eğitimciler öğrenme ilkelerini ve öğrencilerin nasıl öğrendiklerini örtük veya açık bir şekilde bilmelidir. Siemens'e (2005) göre artık ağa bağlı dünya için öğrenme materyallerinin geliştirilmesine rehberlik etmek için dijital çağ için bir teoriye ihtiyaç bulunmaktadır. Eğitimciler, mevcut öğrenme teorilerini dijital çağa uyarlayabilmeli, aynı zamanda etkili öğrenme materyallerinin geliştirilmesine rehberlik etmek için bağlantı prensiplerini kullanmalıdırlar. Siemens'e göre, bağlantıcı kuram, bireylerin ağa bağlı bir ortamda öğrendiği ve çalıştığı dijital çağ içindir. Siemens; bağlantıcı kurama dayanarak öğrenen için öğrenme materyalleri tasarlamaya yönelik bazı yönergeler önermektedir:

1) Bilgi patlaması nedeniyle, öğrencilerin güncel bilgileri keşfetmesine ve araştırmasına izin verilmelidir. Geleceğin öğrencileri özerk ve bağımsız öğrenciler olmalıdır. Böylece geçerli ve doğru bir bilgi tabanı oluşturmak için güncel bilgileri edinebilirler. İnternetin uygun kullanımı ağa bağlı bir dünyada ideal bir öğrenme stratejisidir.
2) Öğrenciler, hangi bilginin artık geçerli olmadığını tanıma yeteneğine sahip olmalıdır. Bu durum, öğrencilerin sahada güncel kalmasını ve öğrenme ağında aktif katılımcılar olmasını gerektirir.
3) Küreselleşme nedeniyle, bilgi konuma özgü değildir ve artan telekomünikasyon kullanımı ile dünyanın dört bir yanından teknoloji uzmanları ve öğrenciler bilgileri paylaşabilir ve gözden geçirebilirler.
4) Dünya telekomünikasyon teknolojisi ile bağlantılıdır. Bu nedenle, öğrenme için bilgi tek bir kaynaktan alınmamalı, ağa bağlı dünyayı ve düşünme çeşitliliğini yansıtacak şekilde birçok kaynaktan toplanmalıdır.
5) Bilgisayar sistemleri alanı öğrenme sürecini değiştirmektedir. Cihazlara yerleştirilen akıllı ajanlar, öğrencilerin nasıl öğrendiklerini ve öğrenme materyallerini nereden aldıklarını etkileyebilmektedir.
6) Bilgi patlaması nedeniyle, geleceğin öğrencileri sürekli yeni bilgi edinmeye istekli olmalıdır. Çevrimiçi öğretim stratejileri, öğrencilere alanda güncel

kalabilmeleri için bir disiplinde yeni bilgileri araştırma ve bulma fırsatı vermelidir.

7) Öğrenciler sürekli olarak öğrendiklerinden ve bilgilerini güncellediklerinden emin olmak için diğer öğrenciler ve uzmanlarla iletişim kurmalıdır.

8) Yenilik ve artan teknoloji kullanımı nedeniyle öğrenme disiplinlerarası bir hale gelmektedir. Öğrencilerin bağlantıları görebilmeleri için farklı disiplinlere maruz kalmaları gerekmektedir.

K-12 düzeyinde harmanlanmış ve tamamen çevrimiçi öğrenme popülerlik kazanmış olsa da çevrimiçi öğrenmenin merkezi bileşeniyle ilgili araştırmaların sınırlı olduğu görülmektedir. K-12 çevrimiçi eğitiminin önemli çoğunluğunun önceden hazırlanmış içerik ve/veya müfredat aracılığıyla verildiği görülmektedir (Basham vd., 2016). Basham vd.'ne göre harmanlanmış veya tamamen çevrimiçi ortamlardaki öğrenciler, tüm öğrenim deneyimleri boyunca bu önceden hazırlanmış materyallerle etkileşime girmektedirler.

Okullarda çevrimiçi içerik oluşturmak için ihtiyaç duyulan zaman ve kaynak yatırımı zaman zaman engelleyici olabilmektedir. Çevrimiçi müfredatın ve disipline özgü içeriğin geliştirilmesi, genellikle yetersiz olan kaynaklara ek yük ve talep getirmektedir. Bunun yerine, materyaller tipik olarak önceden hazırlanmış paket öğrenme ürünlerini daha makul bir maliyetle sunan kurumlar tarafından geliştirilmektedir (Basham vd., 2016). Öğretmenler ise hazır dijital ders ve dijital sistem, belirli dersler, etkinlikler, eşlik eden değerlendirmeler ve sonraki dersin tamamlanması için önceden belirlenmiş yol haritası aracılığıyla öğrenme deneyimini yönlendirmektedirler (Basham vd., 2015; Rice & Carter, 2015).

Çevrimiçi ortamların tasarımı oldukça önemli bir konudur. Evrensel Öğrenme Tasarımı bu noktada dikkat çekmektedir. Evrensel Öğrenme Tasarımı; yalnızca erişimi artırmakla kalmamakta, aynı zamanda öğrenme sürecini de dönüştürebilmektedir. Ancak, bu potansiyelin yerine gelebilmesi için, en başından itibaren esneklik ihtiyacını dikkate alarak Evrensel Öğrenme Tasarımının dikkatli bir şekilde uygulanması gerekmektedir (Rose, 2000). Cast Web Sitesinin (http://www.cast.org) yeniden tasarımı, bu sürecin iyi bir örneği olarak gösterilebilir. Rose öğrenmeye yönelik evrensel tasarımın hem ilkelerini hem de uygulamasını

göstermek için Cast Web Sitesinin tasarlanma sürecini açıklamış; Cast Web Sitesi tasarımcılarının üç soru üzerinden yola çıktıklarını belirtmiştir:

1) Web Sitesinin hedefleri nelerdir?
2) Web ortamları öğrenmenin önündeki hangi engelleri ortaya çıkarır? Kullanıcıların bu engelleri aşmalarına yardımcı olurken hangi bireysel farklılıklar göz önünde bulundurulmalıdır?
3) Web sitesi nasıl değerlendirilmelidir?

Cast Web sitesi için; ziyaretçilerin Evrensel Öğrenme Tasarımı ile ilgili kavramları derinlemesine anlamasını sağlamak ve ziyaretçilere bir organizasyon olarak Cast hakkında derin bir anlayış sağlamak olmak üzere iki ana hedef belirlenmiştir. Cast Web sitesini ziyaret edenler belirli gruplarla sınırlı olmadığı için, farklı becerilere, geçmişlere sahip ve farklı ülkelerden veya kültürlerden gelen birçok farklı türde kullanıcının sistemde yer almasının önemi vurgulanmıştır. Özellikle, engelli kişilerin öğrenim görmesini engelleyecek durumlardan kaçınılması gerekmektedir. Web gibi teknolojiler, tüm öğrenciler için fırsatlar yaratma becerisini artırabileceği gibi yanlışlıkla birçok öğrenciyi dışlama riskini de beraberinde getirebilmektedir (Rose, 2000). Bilgileri tüm kullanıcılara sunmanın mükemmel bir yolu yoktur. Bilgiyi temsil etmenin herhangi bir yolu, bazıları için engeller ve diğerleri için de çeşitli faydalar içerebilir. Öğrenmeye yönelik evrensel tasarımın anahtarı, "herkese uyan tek bir çözüm" yerine alternatifler sunmaktır. Bu bağlamda Cast Web Sitesinin geliştirilme sürecinde de bilgi temsilinin engelleri, etkileşim ve gezinme engelleri ve katılım engelleri için birtakım önlemler alınmıştır (Rose, 2000).

COVID-19 küresel salgın süreci zarfında okullar, bir süre boyunca uzaktan eğitimle faaliyetlerini sürdürmek durumunda kalmışlardır. Lindner vd. (2020) yapmış oldukları çalışma bağlamında uzaktan öğretimi, öğretme ve öğrenme sürecinde eğitmenler ve öğrencilerin fiziksel olarak ayrılması olarak tanımlamaktadır. COVID-19 sürecinde, K-12 öğrencilerinin yeterliliklerine veya uzaktan öğretilme veya öğrenme motivasyonlarına bakılmaksızın uzaktan eğitime mecbur bırakıldığına vurgu yapılmaktadır (Lindner vd., 2020). Wei ve Chou (2020) da yapmış oldukları bir çalışmada çevrimiçi öğrenme ortamlarında öğrenenlerin öz yeterlik algılarının öğrenmeye hazır oluşlarını etkilediği sonucuna ulaşmışlardır. Bahsedilen çalışmada, çevrimiçi öğrenmeye yönelik yüksek düzeyde öz yeterliğe sahip

öğrenciler, düşük düzeyde öz yeterliğe sahip olanlardan daha iyi performans göstermişlerdir.

Reinholz vd. (2020) küresel salgın sebebiyle yüz yüze ortamdan çevrimiçi ortama geçişte öğrenci katılımının önemli ölçüde düştüğünü, ancak eğitmenlerin katılımı artırmak için yeni öğretim stratejileri uygulayabildiğini belirtmektedir. Eğitmenlerin çevrimiçi derslerine adil katılımı teşvik etmek için kullandıkları ve çevrimiçi öğretimlerine dahil edilebilecek yedi somut strateji şu şekildedir (Reinholz vd., 2020):

1) Kullanılacak örnekleri ve standartları yeniden oluşturmak,

2) Öğrenci isimlerini kullanmak,

3) Ara odalar özelliğini kullanmak,

4) Sohbete dayalı katılımdan yararlanmak,

5) Yoklama yazılımı kullanmak,

6) Kapsayıcı bir müfredat oluşturmak,

7) İçeriği kısaltmak.

Çevrimiçi öğrenme ortamlarında öğrenmenin gerçekleşmesi için hem eş zamanlı hem de eş zamansız iletişim kombinasyonunun kullanıldığı öğretim yöntemlerinin ideal olduğu düşünülmektedir. Eş zamansız etkinlikleri desteklemek için eş zamanlı tartışmalar yapmanın avantajlarından biri, yüz yüze bir sınıfın etkileşim deneyimi ile en yakın benzerlik göstermeleridir (Skylar, 2009). Geçmişte eş zamanlı bir etkinlik veya dersin gerçekleştirilebilmesi için video konferans ekipmanlarının yer aldığı sınıflara ihtiyaç duyulurken; günümüzde kişisel bilgisayarlar, cep telefonları ve tabletler gibi pek çok yazılım aracı ile eş zamanlı etkileşim sağlanabilecek hale gelinmiştir. Eş zamanlı bir öğrenme ortamı kullanmanın avantajları arasında bilgi ve öğrenmenin gerçek zamanlı paylaşımı ve soru sormak ve yanıt almak için eğitmene anında erişim yer almaktadır. Bununla birlikte, bu tür bir ortam, toplantı için belirli bir tarih ve saat gerektirir ve bu, çevrimiçi kursların geleneksel olarak teşvik ettiği "her zaman, her yerde" öğrenme vaadiyle çelişmektedir. Eş zamansız kurslar, öğrencilerin akışı önceden kaydedilmiş çeşitli araçları kullanarak kurs içeriğine erişebileceği ve kendi hızında ilerleyebileceği esnek bir ortam sağlar. İletişim ve işbirliği, eş zamansız tartışmalar yoluyla geliştirilir.

Eş zamansız kurslarda öğrenciler iletişim için belirli bir gün/saat ile sınırlı değildir ve öğrencilere bir dizi soruya yanıt hazırlamaları için daha fazla zaman tanınır. Eş zamansız iletişim araçlarına; tartışma gruplarının kullanımı, wiki'ler, bloglar ve e-posta örnek olarak gösterilebilir (Skylar). Eş zamanlı iletişim, öğrencilerin ve öğretmenlerin aynı anda etkileşimde bulunmaları için gerçek zamanlı bir yolken, eş zamansız iletişim gecikmeli zamanda etkileşimi ifade etmektedir. Başka bir deyişle, öğrenciler eş zamansız iletişimde geribildirim için daha fazla zamana sahip olurlar ve çevrimdışı iken yanıtlarını raporlayabilirler (Branon ve Essex, 2001).

Yakın gelecek, yeni salgınlar ve yaklaşan kilitlenmelerle belirsizlikler içerdiğinden, birçok eğitmen eş zamanlı, eş zamansız ve harmanlanmış öğrenme stratejisini içeren üç pedagojik yaklaşımla verilebilecek çevrimiçi eğitimi düşünmek zorunda kalmıştır. Eş zamanlı (aynı zamanlı) çevrimiçi derslerde, öğretim elemanları ve öğrenciler, belirlenen ders saatlerinde bir video konferans yazılımı kullanarak çevrimiçi olarak buluşur ve eğitmenler dersle ilgili dersler verir. Öğrenciler derslere katılır ve sesli olarak veya canlı metin sohbeti yoluyla soru sorabilirler. Eş zamansız (ayrı zamanlı) çevrimiçi derslerde ise, eğitmenler ders videolarını kaydeder ve öğrencilerin en uygun zamanlarında erişebilmeleri için bunları birtakım çevrimiçi ortamlara yükler ve paylaşırlar. Harmanlanmış çevrimiçi öğrenme stratejisi, eş zamanlı ve eş zamansız stratejilerin avantajlarını bir araya getirdiği için en pratik yöntem olarak kabul edilir. Harmanlanmış stratejiyi seçmedeki temel motivasyon, eşzamanlı bir tartışma sırasında sessizce oturmak yerine öğrencinin kendi öğrenme sürecine katılımını artırmaktır. Bununla birlikte, eş zamanlı çevrimiçi sınıf oturumları, geleneksel yüz yüze sınıfın yerini almış bulunmaktadır (Lapitan vd., 2021). Yüz yüze iletişimin hala sanal alternatifinden daha etkili kabul edildiği günümüzde, yüz yüze iletişimin katılımcılar arasında daha yüksek düzeyde güven ve anlayış yaşanmasını sağladığı belirtilmektedir (Burdina vd., 2019). Bu doğrultuda eş zamanlı iletişim ve teknolojilerin kullanımının kısmen de olsa katılımcılar ve eğitmen arasındaki güven ve anlayışı sağlamada etkili olacağı düşünülebilir.

Eş zamanlı (aynı zamanlı) tartışmalar, elektronik posta veya tartışma panosu aracılığıyla bir tartışmayı yönetmeye kıyasla, genellikle kuramsal kavramların daha zengin ve daha derin keşfiyle sonuçlanır. Eş zamanlı öğrenme etkinliklerinde bulunan daha zengin tartışmanın sonucu, öğrencilerin anlamlandırma düzeylerindeki artıştır. Eş zamanlı öğrenme etkinliklerinde geleneksel bir sınıfta

yapıldığı gibi eğitmen tartışmayı olayların sırasını yönetebilmektedir. Daha fazla etkileşimle, öğrencilerin müfredatı, ders beklentilerini anlama ve nihayetinde akademik olarak başarılı olma olasılığı daha yüksektir. Ayrıca, tüm öğrenciler yanıtı gerçek zamanlı olarak duyacağından, eğitmenin belirli bir soruyu eş zamanlı bir ortamda yalnızca bir kez yanıtlaması gerekir. Tamamen eş zamansız bir öğrenme ortamında, öğretim elemanının aynı soruyu derse kayıtlı öğrenci sayısı kadar cevaplamasının gerekebileceği düşünülebilir (Weiler, 2012).

Araştırma kapsamında incelenen kaynaklara yönelik genel bir değerlendirme yapmak gerekirse; öğrencilerin internet ortamında geçirdikleri zamanı da dikkate alarak; çevrimiçi ortamdaki riskler ve tehditler hakkında bilgi sahibi olmalarının ve güvenlik önlemlerini uygulayabilmelerinin önemli olduğu söylenebilir. Bu tez çalışmasında sanal ortamlarda bilgi güvenliği ile ilgili eğitim ihtiyacına dayanarak tasarlanan çevrimiçi ortamın sahip olması gereken özellikler alanyazın kaynaklarına dayanarak belirlenmiştir. Yine öğrencilerin çevrimiçi ortamda almış oldukları eğitime yönelik esaslar; çevrimiçi öğrenmeye yönelik uygulamalar ve öneriler doğrultusunda kararlaştırılmıştır.

İlgili Araştırmalar

Bu bölümde, bilgi güvenliği ve çevrimiçi güvenlik farkındalığına yönelik çalışmalar ile çevrimiçi öğrenmeye yönelik çalışmalar ilgili alt başlıklar dahilinde sunulmuştur.

Bilgi güvenliği farkındalığı ve çevrimiçi güvenlik farkındalığı. İnternet ortamında geçirilen zaman, teknolojinin hayatın her alanına dâhil olması gibi gerekçelerle internet güvenliği, bilgi güvenliği, veri güvenliği, e-güvenlik ve çevrimiçi güvenlik gibi konular önem kazanmıştır. Bahsedilen kavramlar alanyazında birbirlerinin yerlerine kullanılabilmektedir. Bu çalışma kapsamında “bilgi güvenliği” kavramının kullanılması uygun görülmüştür. Bilgi güvenliği konusunda alanyazında yetişkinlere ve farklı yaş gruplarındaki öğrencilere yönelik yapılmış çalışmalara rastlanabilmektedir. Bu bölümde yetişkinler ile ortaöğretim, ortaokul ve ilkokul öğrencilerine yönelik gerçekleştirilmiş çalışmalar sırayla aktarılmıştır.

Rezgui ve Marks (2008) yapmış oldukları bir çalışmada, bilinçlilik, kültürel varsayımlar, inançlar ve sosyal koşullar gibi faktörlerin, üniversite personelinin bilgi güvenliği bilincini etkilediğini ortaya koymakta, bu anlamda çalışılan ortamda

güvenlik bilincini başlatmanın ve teşvik etmenin önemini vurgulamaktadırlar. Aslanyürek de (2016) yetişkinlere yönelik yapmış olduğu bir çalışmada, internet kullanıcılarının internet güvenliği ve çevrimiçi gizlilik alanlarındaki ihlaller karşısındaki kanaatlerini ve farkındalıklarını araştırmıştır. Bu doğrultuda farklı yaş, eğitim ve gelir grubundan gönüllü 479 katılımcıdan anket aracılığıyla veri toplamıştır. Anket soruları katılımcılara Facebook, Twitter, Google Plus gibi sosyal medya platformları üzerinden çevrimiçi ortamda gönderilmiş; katılımcılar ankete yanıt verdikten sonra, anketi diledikleri kişilere aynı ortamlar üzerinden ulaştırmışlardır. Araştırma bulguları, çevrimiçi gizlilik ve güvenlik ihlalleri karşısında internet kullanıcılarının farkındalık boyutunun yüksek olduğunu; fakat bu ihlaller karşısında internet kullanımından vazgeçme eğilimlerinin düşük olduğunu göstermiştir.

Akıllı telefonların bireylerin hayatında ciddi bir yer edindiği gerçeğine dayanarak; Talan vd. (2015) akıllı telefon kullanıcılarının güvenlik farkındalığını belirlemeyi amaçlayarak bir çalışma gerçekleştirmiştir. Araştırmanın çalışma grubunu farklı bölümlerde yükseköğretime devam eden 345 öğrenci oluşturmuştur. Çalışma kapsamında katılımcıların çoğu kişisel verilerinin gizliliğinden endişe duyduklarını; buna rağmen akıllı telefonlarında kişisel verilerini sakladıklarını ancak iş verilerini genellikle saklamadıklarını (%31) belirtmiştir. Katılımcıların çoğunluğunun kötü amaçlı yazılımlardan ve akıllı telefonlar için geliştirilmiş güvenlik yazılımlarından haberdar oldukları ancak bu katılımcılardan sadece yarısının (%59) güvenlik yazılımını akıllı telefonunda kullandığı belirlenmiştir. Yine kullanıcıların çoğunun akıllı telefonlardaki güvenlik kontrollerinden habersiz oldukları tespit edilmiştir. Araştırma kapsamında elde edilen sonuçlardan hareketle, akıllı telefon kullanıcıları için karşılaşılabilecek güvenlik tehditlerine yönelik bilinçlendirme çalışmalarının yapılması önerisi getirilmiştir.

Shillair vd. (2015) yapmış oldukları bir çalışmada bir kullanıcının kişisel sorumluk duygusunun, kullanıcıların kendilerine olan güvenlerinin ve nihayetinde çevrimiçi güvenlik davranışlarının hayata geçirilecek şekilde nasıl eğitileceğini araştırmışlardır. Çalışma kapsamında en savunmasız internet kullanıcıları (değişen çevrimiçi tehditlerle nasıl başa çıkacakları konusunda bilgi sahibi olmayan kullanıcıların) için dahi, kişisel sorumluluk vurgulanarak güvenli çevrimiçi davranışlarla dolaylı deneyimler sağlamanın, onlara güvenlik ipuçları aracılığıyla kendilerini korumanın kolay olduğunu söylemekten daha büyük bir etkiye sahip

olduğu sonucuna ulaşılmıştır. Ayrıca çevrimiçi güvenlik önlemlerine aşina olmayan kullanıcılar için, dolaylı deneyimle birleştirilerek kişisel sorumluluğu vurgulamanın, başkalarının sorumluluğunu vurgulamaktan daha etkili olduğu vurgulanmıştır (Shillair vd., 2015).

Bilgi güvenliği hem kullanıcılar hem de kuruluşlar için önemli bir husustur. Teknoloji bilgi için güvenli bir ortamı garanti edemeyeceğinden; bilgi güvenliğinin insani yönleri, teknolojik yönlerin yanı sıra dikkate alınmalıdır. Safa vd. (2016) yapmış oldukları bir çalışmada, bilgi paylaşımının, işbirliğinin, müdahalenin ve deneyimlerin çalışanların örgütsel bilgi güvenliği politikalarına uyum sağlamaya yönelik tutumlarını önemli ölçüde etkilediği sonucuna ulaşmışlardır. Web tabanlı teknolojiler birçok avantaj sağlamakla birlikte, bilgi güvenliği ihlalleri hala tartışmalı bir konudur. Anti-virüs, güvenlik duvarı, kimlik doğrulama ve izinsiz giriş tespit sistemlerinin hepsi bilgi güvenliğini ele alan teknolojik yönler olmakla birlikte, hiçbiri bilgi için güvenli bir ortam garanti edememektedir (Safa vd., 2016).

Siber suçlara yatkınlık- eğilimin bilgi güvenliği bilinciyle ya da farkındalığıyla ve kişisel faktörlerle ilgili olup olmayacağını araştırdıkları çalışmada Hadlington ve Chivers (2018) 18 ila 84 yaşları arasındaki toplam 1.054 katılımcıya çevrimiçi bir anket uygulamıştır. Katılımcıların toplam %60'ının siber suçlara karşı duyarlılık açısından daha yüksek risk kategorilerinde olduğunu belirtmişlerdir. Siber suçlara yatkınlık açısından daha yüksek risk kategorilerindeki bireyler, daha düşük düzeyde bilgi düzeyine sahip olmanın yanı sıra, daha düşük bilgi güvenliği bilinci sergilemişlerdir. Ayrıca, bazı demografik faktörlerin, yaş ve mevcut istihdam durumu da dahil olmak üzere siber suçlara yatkınlıkla bağlantılı olduğu belirtilmiştir. Bilgi okuryazarlığı, internet bağımlılığı ve sanal aylaklığın sanal zorbalık ile ilişkisinin araştırıldığı bir çalışmada ise; 181 lisans ve lisansüstü eğitimi almış katılımcıdan veri toplanmıştır. Araştırma sonuçlarına göre sanal zorbalığın; internet bağımlılığı ve sanal aylaklık ile pozitif; bilgi okuryazarlığı ile ise negatif yönde anlamlı bir ilişkisinin olduğu tespit edilmiştir. Ayrıca, 25 yaş altı katılımcıların, 35 yaş üstü katılımcılara kıyasla daha fazla sanal zorbalık davranışında bulundukları belirtilmiştir. Araştırmanın bir diğer sonucu ise lisans ve yüksek lisans öğrencilerinin doktora öğrencilerine kıyasla daha fazla sanal zorbalık yaptıkları şeklindedir (Demir & Seferoğlu, 2016).

İş hayatındaki yetişkinlerin ve üniversite öğrencilerinin bilgi güvenliği farkındalığı kadar ortaöğretim, ortaokul ve ilkokul düzeyinde öğrenim görmekte olan öğrencilerin bilgi güvenliği farkındalığı da önem arz etmektedir. Bu hususta ebeveynlerin bilgi güvenliği farkındalığının da çocukları etkileyebileceği düşünülmektedir. Ebeveynlerin bilgi güvenliği farkındalıklarını belirlemek üzere yaptıkları bir çalışmada Karaoğlan-Yılmaz ve Çavuş-Ezin (2017) ebeveynlerin farkındalıklarının belirli bir düzeyde olduğu ancak veri yedekleme konusunda farkındalıklarının düşük olduğu sonuçlarına ulaşmışlardır. Ayrıca ebeveynlerin, çocuklarının bilgi güvenliğini sağlamak amacıyla çocuklarına yeterli bilgi veremedikleri belirlenmiştir. Çalışmada; ebeveynlerin de bilgi güvenliği konusunda yeterli bilgiye sahip olması gerektiği belirtilmiş, ebeveynlerin ve çocukların zarar görmemesi için gerekli kurum ve kuruluşlar aracılığı ile tedbirler alınması ve farkındalık oluşturulmasının gerekliliği vurgulanmıştır. Canbek ve Sağıroğlu (2007) da çocukların ve gençlerin bilgisayar ve internet kullanırken karşılaşabilecekleri güvenlik tehlikelerini araştırdıkları çalışmalarında, eğitmenlerin ve ebeveynlerin konuyla ilgili olarak bilgi sahibi olmaları, çocukların ve gençlerin de konuyla ilgili olarak eğitilmeleri ve takip edilmeleri gerektiğini belirtmişlerdir.

Çocukların ve gençlerin internet ortamındaki tehlikelere yönelik bilgi sahibi olması önemlidir. Bilgi güvenliği farkındalığı ve bilincine ilişkin Güldüren vd. (2016) ortaöğretim öğrencilerinin bilgi güvenliği farkındalık seviyelerini belirlemek amacıyla bir ölçek geliştirmişlerdir. Yapılan açımlayıcı faktör analizi (AFA) sonucunda, ölçeğin 36 madde ve 3 alt boyuttan (saldırı ve tehditler, mahremiyet ile kişisel verilerin korunması) oluştuğu belirlenmiş, doğrulayıcı faktör analizi sonuçları ile de yapının doğrulandığı tespit edilmiştir. Geliştirilen ölçek aracılığıyla elde edilen sonuçlar; öğrencilerin bilgi güvenliği farkındalıklarına ilişkin ortalama puanlarının, cinsiyete bağlı olarak anlamlı bir farklılık gösterdiğini göstermiştir. Öğrencilerin bilgi güvenlik farkındalığı davranışlarını etkileyen faktörlere yönelik yapmış oldukları bir çalışmada Rençber ve Mete (2017) ise şifre yönetiminin, mobil internet kullanımının, e posta ve internet kullanımının ve sosyal ağ sitelerinin kullanım davranışlarının bilgi güvenlik farkındalığını en çok etkileyen faktörler olduğu belirtmiştir.

İlköğretim ve ortaöğretim öğrencilerinin bilgi güvenliği farkındalık düzeylerini ve etkili değişkenleri belirlemek amacıyla gerçekleştirmiş oldukları çalışmalarında Tekerek ve Tekerek (2013) öğrencilerin etik konularında yeterli bilinç düzeyine sahip

olduklarını ancak kurallar ve bilgi gerektiren konularda farkındalık düzeylerinin ise düşük olduğunu tespit etmiştir. Bu sonuç, bilgi ve bilgisayar güvenliği farkındalık eğitim ve etkinliklerinin yetersiz kaldığı şeklinde yorumlanmıştır. Çalışmada öğrencilere, öğretmenlere ve velilere yönelik eğitim faaliyetleri düzenlenerek bilgi güvenliği farkındalık düzeylerinin artırılabileceğine yönelik öneri getirilmiştir. Kaşıkçı vd. (2014) de, Avrupa Çevrimiçi Çocuklar projesine katılan Türkiye ve 23 Avrupa ülkesinin bulgularını inceleyerek gerçekleştirdikleri çalışmaları kapsamında; ebeveyn ve çocukların okul, internet servis sağlayıcıları, bilgisayar firmaları ve sivil toplum kuruluşları tarafından bilgilendirilmesi gerektiğini belirtmişlerdir.

Çocukları çevrimiçi mahremiyetin yönetimi konusunda eğiten bir oyunun tasarım sürecinin ve sonuçlarının araştırıldığı bir çalışmada; tasarlanan oyunun öğrenme amacının, oyuncuların günlük yaşamdaki mahremiyet risklerini değerlendirme ve ne zaman, neye ve kime güvenecekleri konusunda uygun kararlar verme yeteneklerini artırmak olduğu belirtilmiştir (Raynes-Goldie & Allen, 2014). Oyundan önce ve sonra yapılan tartışmalar ve oyunun test oturumları sırasında gözlem yoluyla birlikte doğrudan geri bildirim alarak oyunun tasarımı ve başarısı hakkında fikir edinilmiştir. Oyunun tasarım sürecinde, çocukların mahremiyet odaklı davranışları öğrenmelerinin bir aracı olarak sosyal etkileşimin ve işbirlikçi değerlendirmenin yararlı olduğuna dair güçlü bir anlayışa sahip oldukları bulgusuna ulaşılmıştır. Yine; çocukların akranlarla etkileşime önemli bir problem çözme tekniği olarak değer verdikleri belirtilmiştir. Çalışma sonucunda, çocukları öğrenme sürecinde ortaklar olarak kabul etmenin, çocukların çevrimiçi ortamda kendilerini nasıl güvende olabileceklerini anlamalarına katkı sağlayacağına vurgu yapılmıştır.

Bilgi güvenliği kavramı ile güvenli internet kavramları benzer kavramlardır. Beder ve Ergün (2015) ortaokul öğrencilerinin güvenli internet kullanım durumlarını araştırdıkları çalışmalarında, öğrencilerin “telif hakkı ihlali” ve “sorun olabilecek paylaşımlar” ile ilgili bilinç seviyelerinin düşük olduğu, “yazılımsal tehditler” ile ilgili kararsız kaldığı durumlar olduğunu belirlemişlerdir. Çalışma sonucunda, ortaokul öğrencilerinin bilinç seviyelerinin artırılabilmesi amacıyla, çocuklara güvenli internet kullanımı ile ilgili bilinçlendirmeye yönelik eğitsel çalışmaların planlanması önerisi getirilmiştir. Gökçearslan ve Seferoğlu (2016) da ortaokul öğrencilerinin internet kullanım biçimlerini araştırdığı çalışmasında; öğrencilerin çeşitli riskli davranışları sergilemekte olduklarına; cinsiyet, anne öğrenim durumu değişkenlerinin, riskli

İnternet davranışları ile ilişkili olduğu sonuçlarına ulaşmışlardır. Bu doğrultuda öğrencilere, ailelere ve çeşitli kurumlara çevrimiçi riskler konusunda sorumluluk düştüğü, paydaşların işbirliği ile sorunların çözülebileceği belirtilmiştir.

Kullanıcılara sunulan çok sayıda güvenlik tavsiyesi ve çevrimiçi eğitim materyali olmasına rağmen, güvenlik davranışları için geliştirilen standart bir araç bulunmamaktadır (Egelman & Peer, 2015). Egelman ve Peer, kullanıcı güvenlik davranışlarını belirlemek amacıyla "güvenlik davranışı niyetleri" ölçeğini geliştirmişlerdir. Bu amaçla; uzmanların bilgisayar kullanıcılarına sundukları tavsiyeleri incelemiş ve bir dizi likert tür soru oluşturmuşlardır. Çalışmada 3619 bilgisayar kullanıcısına sunulmuş olan soru setinin hem açımlayıcı hem doğrulayıcı faktör analizleri yapılmış olup; 4 alt temadan oluşan 16 maddelik bir ölçek oluşturulmuştur. Ölçeğin alt temaları; cihaz güvenliği, şifre üretimi, proaktif farkındalık, güncelleme yapma şeklinde belirlenmiştir.

Bilgi güvenliği sadece toplumun belirli bir kesimi için değil; toplumu oluşturan her birey için önemlidir. Bu kapsamda alanyazında dikkat çeken bir kavram da siber sağlıktır. Mıhçı Türker ve Kılıç Çakmak (2019) siber sağlık kavramından söz ederek; siber sağlığı belirleyebilmek amacıyla internet bağımlılığı, çevrimiçi nezaket, çevrimiçi mahremiyet, çevrimiçi uygunsuz içerik, siber zorbalık, telif hakkı ve çevrimiçi güvenlik olmak üzere toplam yedi ölçek geliştirmişlerdir. Araştırmada, öğrencilerin internet bağımlılığı, siber zorbalık, çevrimiçi mahremiyet ve çevrimiçi güvenlik konularında yüksek düzeyde ancak çevrimiçi nezaket, çevrimiçi uygunsuz içerikler ve telif hakkı konusunda ise orta düzeyde farkındalığa sahip oldukları belirlenmiştir. Bunun yanı sıra, öğrencilerin farkındalık düzeyleri, çeşitli değişkenler açısından incelenmiştir. Bu doğrultuda, cinsiyet, öğrenim görülen ilçe, sınıf düzeyi, internet kullanım süresi, değişkenlerine bağlı olarak farkındalık düzeyinde anlamlı bir farklılık belirlenememiştir. Öğretmenlerin siber sağlığa yönelik farkındalık düzeylerinin, orta düzeyde olduğu belirlenmiş olup, öğretmenlerin farkındalık düzeyleri görev yaptıkları ilçeler ve eğitim alma isteklerine bağlı olarak farklılaşmıştır. Mıhçı Türker ve Kılıç Çakmak, çalışmaları kapsamında velilerin çocuklarının siber sağlık düzeylerine yönelik görüşlerini de değerlendirmiştir. Bu doğrultuda, veliler, çocuklarının internet bağımlılığı, çevrimiçi nezaket, çevrimiçi mahremiyet, çevrimiçi uygunsuz içerikler, telif hakkı ve çevrimiçi güvenlikler

konusunda orta düzeyde; siber zorbalık konusunda ise yüksek düzeyde farkındalığa sahip olduklarını düşündüklerini belirtmişlerdir.

Zilka (2017) yapmış olduğu bir çalışmada, çocukların ve gençlerin perspektifinden internet kullanımının iyi veya kötü yönlerini açıklamıştır. Çalışma kapsamında yaşları 8-18 arasında değişen 345 öğrenciden veri toplanmıştır. Veri toplama aracı olarak ölçek ve görüşmeden faydalanılmıştır. Bu doğrultuda; çocukların ve gençlerin interneti kullanımının doğasını ve çocukların çevrimiçi tehlikelerle başa çıkmak için araçlara ihtiyaç duyup duymadıklarını tespit etmek amaçlanmıştır. Bu amaç doğrultusunda 10 çoktan seçmeli, üç açık uçlu sorudan oluşan E-güvenlik farkındalığı ölçeği uygulanmıştır. Ölçekte çoktan seçmeli sorular; güvenli internet kullanımının unsurları hakkında farkındalık ve çevreye danışma ihtiyacı olmak üzere iki faktörde toplanmıştır. Açık uçlu sorularda ise; "kişisel verileri paylaşmama, bilgi ve öz düzenleme, boş zaman aktiviteleri ve oyunlar, teknik sınırlılıklar, kişisel verilerin ifşa edilmesi ve kişisel zarar, siber zorbalık, uygun olmayan içeriğe maruz kalma ve cinsel saldırı, öz düzenleme ve öz kontrol, farkındalığın geliştirilmesi ve eğitim, interneti engellemek ve bilgisayarı korumak ile kişisel verileri paylaşmaktan sakınmak" temaları elde edilmiştir. Bu veriler doğrultusunda ölçek, güvenli internet kullanımı (Tanıdıklık temelinde iletişim, kişisel verilerin paylaşımından kaçınma, bilgi ve özdenetim, teknik sınırlama, oyun, boş zaman aktiviteleri ve sosyalleşme); çevrimiçi tehlikeler (Kişisel verilerin ifşası ve kişisel zarar, cinsel saldırılar, siber zorbalık ve cinsel olmayan saldırılar, uygunsuz içeriklere maruz kalma); çevrimiçi tehlikelerden kaçınma (Kişisel aşinalık temelli olmayan temastan kaçınma, kişisel verilerin açıklanmasından kaçınma, internetin engellenmesi ve bilgisayarın korunması, öz düzenleme ve öz denetim, artan farkındalık ve eğitim) temalarıyla tekrar düzenlenmiştir.

Çevrimiçi öğrenme ve bilgi güvenliği eğitimi. Çevrimiçi risklerin çoğalması ve bu risklerin bireyler için tehdit haline gelmesiyle birlikte, işyerlerinde ve okullarda bilgi güvenliği, siber güvenlik, veri güvenliği ve çevrimiçi güvenlik farkındalığına yönelik yüz yüze ve çevrimiçi ortamda eğitimler gerçekleştirildiği görülmektedir. Bu bölümde yetişkinler ile ortaöğretim, ortaokul ve ilkokul öğrencilerine yönelik gerçekleştirilmiş çalışmalar sırayla aktarılmıştır.

Çevrimiçi eğitim; uzaktan iletişim, sanallaştırma ve eş zamansız katılımda teknik kapasiteler nedeniyle ekipler veya daha küçük öğrenci grupları için zaman ve

mesafe sınırlarının ötesinde işbirliğine dayalı öğrenme açısından büyük bir potansiyel sunmakla birlikte birtakım zorluklar da içerebilmektedir. Örneğin, ekip oluşturma ve geliştirmede başarılı işbirliğinin, ekip çalışması için motivasyonun, ekip ve bireysel değerlendirme ve çatışma yönetimi için sanal ekiplerin ve grupların uygulanmasının önünde engeller olabilmektedir (Lilian, 2014; Chiong & Jovanovic, 2012; Roberts & McInnerney, 2007).

K–12 ve yüksek eğitimde, çevrimiçi ve yüz yüze eğitimin etkinliğinin yeniden gözden geçirilmesi gerekmektedir. Web tabanlı uygulamaların ve işbirliği teknolojilerinin artan yetenekleri ve web tabanlı ve yüz yüze sınıf eğitimini birleştiren karma öğrenme modellerinin yaygınlaşması, çevrimiçi öğrenmenin etkinliği için beklentileri artırmıştır (Means vd., 2009). Means vd. tamamen çevrimiçi veya harmanlanmış öğrenme koşulları için öğrenme çıktılarını yüz yüze sınıf öğretimiyle karşılaştıran çalışmaların istatistiksel bir sentezini üretmek için bir metaanaliz çalışması gerçekleştirmişlerdir. Analiz sonuçları, çevrimiçi öğrenme koşullarındaki öğrencilerin ortalama olarak yüz yüze eğitim alanlara göre daha iyi performans gösterdiğini ortaya koymuştur. Araştırma ayrıca, karma öğrenmeyi kullanan çalışmaların, öğrenciler arasındaki etkileşimi teşvik eden ek öğrenme zamanını, öğretim kaynaklarını ve ders ögelerini içerdiği belirtilmiştir. Bu durumun, harmanlanmış öğrenme için özellikle olumlu sonuçlara katkıda bulunma olasılığını ortaya koyduğu açıklanmıştır.

Alanyazın incelendiğinde gerek yetişkinler gerekse K-12 okullarında öğrenim görmekte olan öğrencilere yönelik çevrimiçi güvenlik eğitimleri dikkat çekmektedir. Skylar vd. (2005) yapmış oldukları bir çalışmada, çeşitli öğretim ortamları ve yöntemlerinin kullanıldığı üç özel eğitim kursuna katılan öğrencilerin başarı, öğrenci memnuniyeti ve öğretim üyesi ders değerlendirmelerini araştırmıştır. Araştırma kapsamında; geleneksel bir sınıf, bir çevrimiçi sınıf (WebCT) ve bir multimedya CD-ROM'ları aracılığıyla bir sınıfta kurslar gerçekleştirilmiştir. Öğretim içeriğini sunmak için PowerPoint notları, ders notları, dijital videolar ve ders kitabı gibi çeşitli materyaller kullanılmıştır. Çalışmanın sonuçları, öğrencilerin başarısı ile üç koşul (örneğin., geleneksel sınıf, çevrimiçi sınıf veya multimedya CD-ROM'ları aracılığıyla bir kutuda sınıf) arasında önemli bir fark bulunmadığını ortaya koymuştur. Ayrıca, üç grup için öğrenci memnuniyeti açısından da anlamlı bir farklılık bulunmamıştır.

Bütün gruplardaki öğrenciler katıldıkları eğitim medyasının türünden memnun olduklarını belirtmişlerdir (Skylar vd., 2005).

Siber güvenlik gibi teknolojiyle ilgili kariyer alanları için gerekli teknik becerilere veya zor becerilere ek olarak, ekip çalışması, iletişim ve iş etiği gibi beceriler, günümüzün iş yerinde başarı için gereken en önemli sosyal beceriler arasındadır (Wang, 2017). Siber güvenlik eğitimlerinde yetişkinler için çevrimiçi ortama sıklıkla başvurulduğu bilinmektedir. Ancak günümüzde çevrimiçi ortam aracılığıyla verilen eğitimler K-12 okullarında öğrenim görmekte olan öğrenciler için de tasarlanmaktadır. Padlipsky (2018) siber güvenlik eğitiminin etkinliğini arttırmak amacıyla hazırlamış olduğu çalışmasında; siber güvenlik alanındaki çevrimiçi bir kursun, geleneksel sınıf yöntemlerini yansıtan çevrimdışı, yüz yüze yapılan etkinliklerle geliştirilip geliştirilemeyeceğini araştırmıştır. Sonuçlar, kursun hem çevrimiçi hem de çevrimdışı kısımlarına katılan grubun siber güvenliğe karşı daha olumlu bir farkındalığa sahip olduğunu göstermiştir.

Siber zorbalık müdahale ve önleme programlarının etkinliğinin sistematik incelemesinin yapıldığı bir araştırmada 2000'den 2017'nin sonuna kadar belirli dergilerdeki çalışmalar taranmış; 192 çalışma değerlendirmeye alınmıştır (Gaffney vd., 2019). Araştırma sonuçları; siber zorbalıkla mücadele programlarının siber zorbalık suçunu yaklaşık %10-15 ve siber zorbalık mağduriyetini yaklaşık %14 oranında azaltabileceğini göstermektedir. Genel olarak, bahsedilen çalışmanın kapsamının müdahale ile siber zorbalık ve mağduriyeti önlemenin etkili olabileceğini öne sürdüğünü söylemek mümkündür.

Tsim (2006) California'daki bir ortaokulda öğrenim görmekte olan 7. ve 8. Sınıf öğrencilerine yönelik çevrimiçi davranış ve riskler konulu sunumlar aracılığıyla internet güvenliği eğitimi vermiş, bu eğitimin etkililiğini araştırmıştır. Bu bağlamda; internet güvenliği davranışlarında en fazla gelişmenin evde internet erişimi olan ortaokul öğrencilerinde görüldüğü bilgisine, erkek öğrencilerin kız öğrencilere kıyasla daha fazla riskli çevrimiçi davranışlarda bulunduğu sonuçlarına ulaşılmıştır. Jones vd. (2014) de ABD'deki gençlerin neredeyse yarısının, okullarında internet güvenliği eğitimi aldığını; ancak siber zorbalık, cinsel içerikli mesajlaşma veya çevrimiçi saldırganlar gibi sorunlarda hangi eğitim mesajlarının fark yarattığı hakkında çok az şey bilindiğini belirtmişlerdir. Jones vd., yapmış oldukları bir çalışmada, dört internet güvenliği eğitimi programından alınan materyaller üzerinde

bir içerik analizi gerçekleştirmişlerdir. Elde edilen sonuçlar internet güvenliği eğitimi programlarının çoğunlukla kanıtlanmış eğitim stratejilerini içermediğini göstermiştir. Bu bağlamda; program geliştiricilerin ve diğer paydaşların internet güvenliği eğitimi mesajlarını yeniden gözden geçirmeleri, eğitim stratejilerini geliştirmeleri ve değerlendirmeye katılmaları önerilmiştir. Yine; internet güvenliği eğitimi uzmanları için öğrettikleri belirli elektronik ortam becerilerini daha geniş eğitim ve önleme programlarına entegre etmeleri tavsiye edilmiştir (Jones vd., 2014).

Uzaktan eğitim, bazı sebeplerle okula gitme fırsatı bulamayan öğrenciler açısından fırsatlar sağlayabilir. Burdina vd. (2019) yapmış oldukları bir çalışmada, ilkokul için çok yönlü bir uzaktan eğitim programı geliştirmiş ve programın etkililiğini test etmişlerdir. 8-9 yaşlarında 430 öğrencinin katıldığı çalışmada; öğrencilerin daha iyi notlar almak için yalnızca kolaylaştırıcılara değil, aynı zamanda onlara rehberlik eden bir öğretmene de ihtiyaçları olduğuna dikkat çekilmiştir. Yine öğrenci-öğretmen iletişiminin, öğrencilerin akademik performanslarını ve motivasyonlarını yükseltmelerine yardımcı olabileceği vurgulanmıştır. Araştırma sonuçları; öğrencilerin zamanında sorduğu soruların, sınıfın akademik düzeyine ulaşamayan öğrencilerin sayısını %9'dan %0'a düşürürken; başarılı olarak nitelendirilebilecek öğrenci sayısını %11'den %26'ya çıkardığını göstermiştir.

Çocukların e-güvenlik becerilerini geliştirmek için etkileşimli bir web tabanlı öğrenme ortamının etkililiğini değerlendirmek amacıyla yürütülen bir çalışmada; geliştirilen web tabanlı öğrenme ortamını kullanan 48 altıncı sınıf öğrencisinden oluşan bir deney grubu ve 25 kişilik bir kontrol grubu ile yarı deneysel ön test son test kontrol grup tasarımı kullanılmıştır. Tutum anketinin ve öğrenci görüşmelerinin analizi, deney grubu öğrencilerinin öğrenme ortamına yönelik olumlu tutumları olduğuna yönelik katınlar sağlamıştır. Elde edilen araştırma sonuçları; çocukların e-güvenlik becerilerini geliştirmek için hem örgün eğitimde hem de yaygın öğrenme ortamlarında kullanılabilen web tabanlı öğrenme ortamının etkili olduğu şeklinde yorumlanmıştır (Nicolaidou & Venizelou, 2020).

Öğrenilenlerin kalıcılığı. Öğrencilerin çevrimiçi ortamda güvenli davranışlar sergileyebilmesi; çevrimiçi ortamdaki risklerin farkında olmaları ve güvenlik önlemlerini bilmelerinin yanı sıra, öğrenilenlerin kalıcılığının sağlanması ile ilişkilendirilebilir.

Alanyazın incelemesi yapıldığında; bilgi güvenliği konusunda verilen eğitimlerin kalıcılığına yönelik yeterli çalışmaya rastlanmamıştır. Bu bölümde; öğrenilenlerin kalıcılığının sağlanması amacıyla çevrimiçi teknolojiler aracılığıyla farklı disiplinlere yönelik olarak gerçekleştirilmiş çalışmalara yer verilmiştir.

Google Apps Eğitim Sürümü ve diğer bulut bilişim teknolojilerine dayalı bazı yenilikçi eğitim araçlarına yönelik bir incelemenin yapıldığı bir araştırmada; Google Formlar ile entegre eğitici video kanalının öğretmenlere; öğrencilere bilgiyi kalıcı olarak öğretebilecekleri yenilikçi öğrenme tekniklerini kullanma imkânı tanıdığına vurgu yapılmaktadır (Dmitriev vd., 2012).

Etkileşimli öğrenci yanıt sistemi, öğrencinin ders ve sınav performansını iyileştirme potansiyeline sahip alternatif bir öğrenme yöntemidir (Chui vd., 2013). Etkileşimli öğrenci yanıt sistemi kullanımı ile ders performansı arasındaki ilişkiyi incelemek amacıyla gerçekleştirilen bir araştırma kapsamında; etkileşimli öğrenci yanıt sisteminin öğrencilerin sınıf içi kısa sınav (quiz) performansını geliştirdiğine dair sonuçlar elde edilmiştir. Çalışma kapsamında ileride yapılacak araştırmalar için etkileşimli öğrenci yanıt sistemine dayalı olarak derin ve kalıcı öğrenmenin oluşup oluşmadığının araştırılması önerilmiştir (Chui vd., 2013).

Lise öğrencilerine yönelik olarak geliştirilen mobil uygulamanın; öğrencilerin kimya dersi akademik başarılarına, kalıcı öğrenmelerine ve motivasyonlarına etkisinin araştırıldığı bir çalışmada; yarı deneysel desenden faydalanılmıştır. Çalışma sonuçlarına göre mobil uygulamayı kullanan öğrencilerin kimya dersi atom ve periyodik sistem ünitesindeki akademik başarılarının mobil uygulamayı kullanmayan öğrencilere göre daha yüksek olduğu belirlenmiştir. Mobil uygulamayı kullanan öğrencilerin mobil öğrenmeye karşı tutum puanları ve kalıcılık puanlarının uygulamayı kullanmayan öğrencilere göre daha yüksek olduğu tespit edilmiştir (Kılıç, 2015). Öğrencilere basit elektrik devreleri konusunda verilen problemlerin çözümü için Scratch programlama ortamında kendi kodlamalarıyla geliştirdikleri simülasyon benzeri etkinlikler aracılığıyla eğitimin verildiği bir çalışmada ise; Scratch programlama ortamı kullanılarak gerçekleştirilen aktif öğrenme ortamının kalıcı öğrenme açısından etkisi araştırılmıştır. Araştırma kapsamında kullanılan yarı yapılandırılmış görüşme formu bulguları, öğrenenlerle gerçekleştirilen aktif öğrenme yönteminin görsel içerikler barındırarak kalıcı öğrenmeyi desteklediğini göstermiştir (Akpınar, 2019).

Zeybek (2020) bilgisayar destekli zihin haritası kullanımının öğrenilenlerin kalıcılığı üzerindeki etkisini belirlemek amacıyla yapmış olduğu çalışmasında; kendi geliştirilmiş olduğu başarı testi ve öğrenciler tarafından hazırlanan öğrenme günlüklerini kullanmıştır. Araştırmanın nicel sonuçları, öğrenilenlerin kalıcılığını sağlamada bilgisayar destekli zihin haritası kullanımının başarılı olduğunu göstermiştir. Araştırmanın nitel sonuçlarına göre ise; bilgisayar destekli zihin haritası uygulamasının öğrenciler tarafından ilgi çekici olarak görüldüğü; öğrenmeyi kolaylaştırdığının ifade edildiği belirlenmiştir. Ortaokul öğrencilerinin eğitsel çevrim içi sosyal öğrenme ortamı Edmodo'nun erişiye ve kalıcılığa etkisinin araştırıldığı bir çalışmada ise; 6.sınıfta öğrenim görmekte olan 192 öğrenci ile deneysel bir çalışma yürütülmüştür. Deney grubundaki öğrencilere, fiziksel uygunluk kavramları Edmodo aracılığı ile öğretilmiş; bu kavramların uygulamasına yönelik çalışmalar spor salonunda yaptırılmıştır. Kontrol grubundaki öğrencilere ise aynı kavramlar spor salonunda sözlü anlatım yolu ile aktarılmış ve uygulamalar gerçekleştirilmiştir. Araştırma sonuçları; Edmodo ile zenginleşen öğrenme ortamının, deney grubundaki öğrencilerin erişilerine olumlu etkisinin olduğunu, ayrıca öğrenmenin kalıcılığı bağlamında önemli bir katkı sağladığını göstermiştir (Bulca & Demirhan, 2020).

İlgili Araştırmalar Özet

İncelenen alanyazın bilgi güvenliği ve çevrimiçi güvenlik konularına yönelik farklı yaş düzeyindeki öğrencilerin eğitim ihtiyacına dikkat çekmektedir. Özellikle COVID-19 küresel salgın sürecinde çevrimiçi ortamda alınan eğitimler aracılığıyla çocukların internette geçirdikleri zamanın artması, birtakım çevrimiçi riskler ve tehditleri de beraberinde getirmiştir.

Çocukların ve gençlerin bilgisayar ve internet kullanırken karşılaşabilecekleri güvenlik tehlikeleri hakkında bilinç ve farkındalık kazanmalarının önemi pek çok çalışmada vurgulanmaktadır. Çocukların çevrimiçi ortamlarda pek çok riske maruz kalmalarının özellikle ebeveynler açısından endişe kaynağı olduğu görülmektedir. Küresel salgın koşullarında eğitimin de çevrimiçi ortama taşınmasıyla beraber, çocukların çevrimiçi ortamlarda karşılaşabilecekleri tehlikeler ve riskler konusunda bilgi ve farkındalık sahibi olmaları konusu tekrar gündeme gelmiştir. Bu bağlamda; çocukların çevrimiçi ortamda nasıl güvende olabileceklerini anlamalarını sağlayacak etkinliklere ihtiyaç duyulmaktadır.

Alanyazında, öğrencilere yönelik eğitim faaliyetleri düzenlenerek öğrencilerin bilgi güvenliği farkındalık düzeylerinin artırılabileceğine yönelik önerilere rastlanmaktadır. Örneğin akıllı telefon kullanıcıları için; karşılaşılabilecek güvenlik tehditleri, veri gizliliği, çevrimiçi mahremiyet konularına yönelik bilinçlendirme çalışmalarının yapılması önerileri dikkat çekmektedir.

Siber suçlara yatkın olduğu düşünülen bireylerin, daha düşük düzeyde bilgi düzeyine sahip oldukları ve daha düşük bilgi güvenliği bilinci sergiledikleri; çevrimiçi güvenlik önlemlerine aşina olmayanlar kullanıcılar için dahi kişisel sorumluluğu vurgulamanın etkili olduğu düşünülmektedir. Bu hususlar bağlamında yine öğrencilere yönelik eğitim faaliyetlerinin ihtiyacının önem kazandığı söylenebilir. Siber güvenlik, internet güvenliği ve çevrimiçi güvenlik konularında eğitimlere yönelik yapılan araştırmalar farkındalık düzeyinin artmasıyla beraber; genellikle siber zorbalık yapma ve mağdur olma oranlarının ve karşılaşılabilecek diğer çevrimiçi risklerin azaltılabileceğine yönelik bulgular sunmaktadır.

Uzaktan eğitim ya da çevrimiçi eğitim, bazı sebeplerle okula gitme fırsatı bulamayan öğrenciler açısından fırsatlar sağlayabileceği gibi öngörülmesi mümkün olmayan küresel salgın koşullarında da öğrenciler açısından birtakım fırsatlar ve avantajlar sağlayabilmiştir. Örneğin, yüz yüze eğitim koşullarında öğretmeniyle yeterince diyalog fırsatı bulamayan öğrenciler, eş zamansız ve eş zamanlı olmak üzere farklı tekniklerin kullanılabildiği çevrimiçi ortamlarda bilgiye erişim ve diyalog açısından avantajlar elde edebilmişlerdir.

Öğrencilerin öğrenme deneyimi kazanmasına katkı sağlayabilecek çevrimiçi öğrenme ortamlarının kalıcı öğrenme açısından etkili olduğu alanyazında pek çok çalışmanın sonuçlarında vurgulanmaktadır. Özellikle öğrenenlerin, bilgiye erişim açısından farklı seçeneklere sahip olabileceği, etkinlikler aracılığıyla da aktif katılım sağlayabileceği ortamların kullanımının öğrenmenin kalıcılığı açısından etkili olabileceğini söylemek mümkündür.

Günümüzde çocukların internet ile çok erken yaşlarda tanıştığı gerçeğinden hareketle çevrimiçi ortamdaki güvenlik ve risk faktörlerinin önemi dikkate değer olmaktadır. Yine, internete erişimin artık sadece okullarda olmaması gerçeği; çocukların günlük hayatta çevrimiçi ortamda karşılaşabilecekleri risklerin farkına

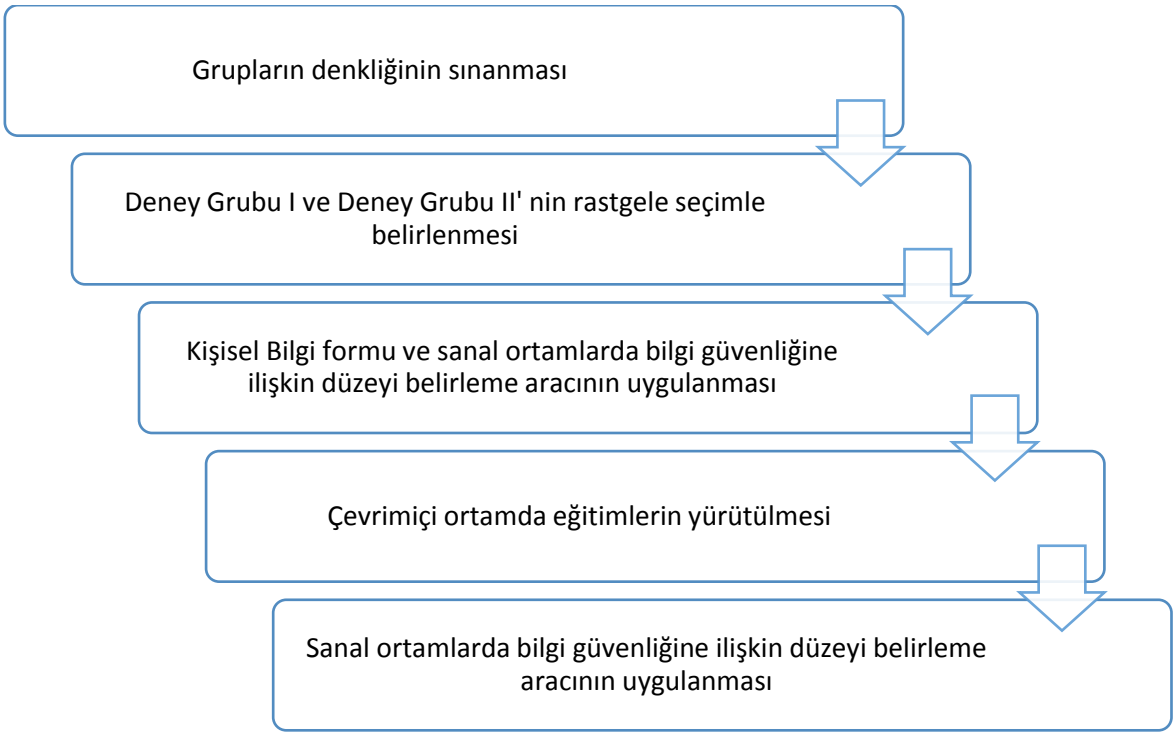
varması ve güvenli kullanıma yönelik bilgi edinmesi konularını gündeme getirmektedir.

Alanyazında yer alan öneriler ve bilgiler doğrultusunda tasarlanan çevrimiçi bir ortamda verilen bilgi güvenliği eğitimlerinin etkililiğinin araştırılmasına karar verilmiştir. Bu çalışmada; küresel salgın koşullarında evlerinden eğitim görmekte olan öğrenciler sanal ortamlarda bilgi güvenliği eğitimi konusuna yönelik hazırlanmış bir çevrimiçi ortam aracılığı ile eğitimlere katılma deneyimini yaşamışlardır. Tasarlanan ortam, öğrencilerin ihtiyaçlarını dikkate alarak eş zamansız olarak erişebilecekleri şekilde içerik ve etkinlikler sunulmasına imkân tanıyan güvenli bir eğitim ortamı sağlamıştır.

Bölüm 3.
Yöntem

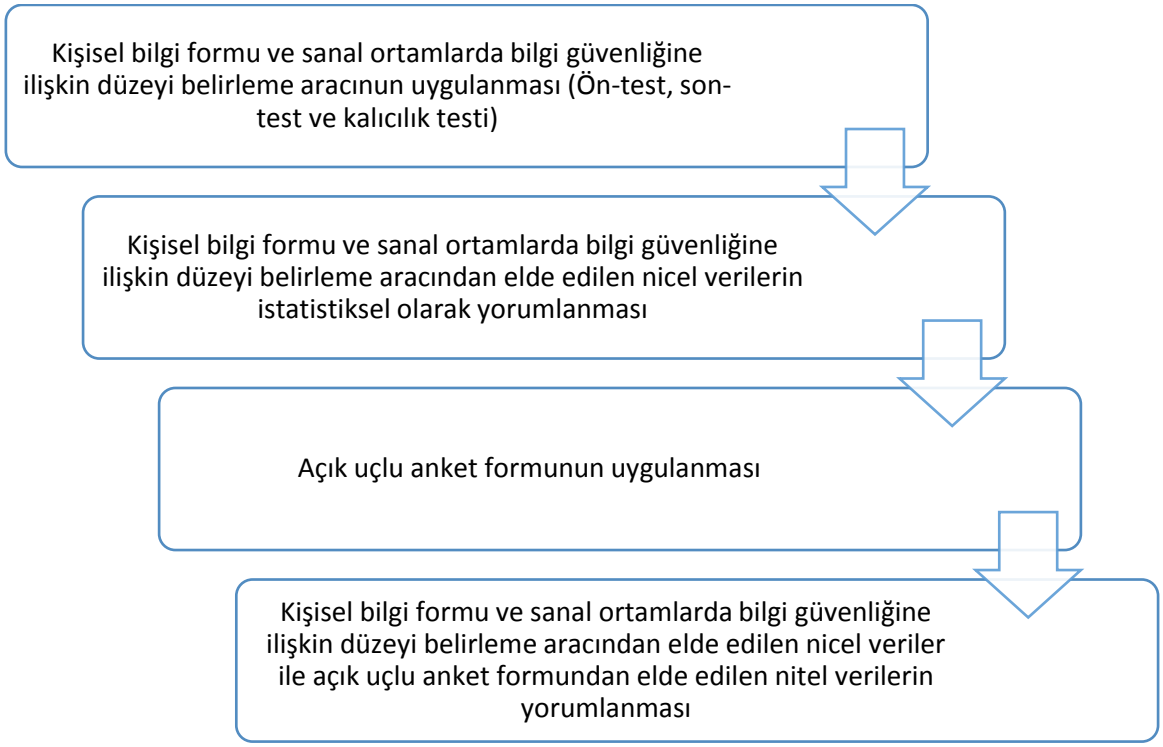
Bu araştırmada nicel araştırma yöntemlerinden yarı deneysel desen kullanılmış, araştırma nitel verilerle de desteklenmiştir.

Araştırmanın çalışma grubunu Ankara ilinde merkezi bir ortaokulda 6.sınıfta öğrenim görmekte olan öğrenciler oluşturmaktadır. Araştırmanın pilot uygulama ve asıl uygulama süreçleri farklı çalışma grupları ile yürütülmüştür. Pilot uygulama sürecinde nicel verilerin toplandığı aşamada zayıf deneysel desenlerden tek grup ön test son test deseninden faydalanılmış; açık uçlu bir anket formu ile toplanan nitel verilerle araştırma bulguları desteklenmiştir. Tek grup ön test-son test deseninde, deneklerin bağımlı değişkene ilişkin ölçümleri uygulama öncesinde ön test, uygulama sonrasında son test olarak aynı denekler ve ölçme araçları kullanılarak elde edilmektedir (Büyüköztürk vd., 2020). Asıl uygulama sürecinde ise pilot çalışmadan farklı olarak nicel verilerin toplandığı aşamada statik grup ön test son test deseninden faydalanılmıştır. Statik grup ön test son test deseninde, gruplardaki deneklerin uygulama öncesinde bağımlı değişkene ait ölçümleri elde edilmektedir (Büyüköztürk vd., 2020). Asıl uygulama sürecinde de pilot uygulama sürecine benzer bir şekilde nicel aşamada elde edilen verileri açıklamak amacıyla açık uçlu anket formları verilerinden faydalanılmıştır. Araştırma deseninin şematik gösterimi Şekil 1'de sunulmuştur:



Şekil 1. Araştırma desenine yönelik şematik model

Araştırmanın verilerinin yorumlanabilmesine yönelik şematik gösterim Şekil 2'de sunulmuştur:



Şekil 2. Araştırmanın verilerinin yorumlanabilmesine yönelik şematik model

Araştırmanın pilot uygulama süreci için deneysel desen ve işlemler Tablo 1'de verilmiştir.

Tablo 1

Pilot Uygulama Süreci İçin Deneysel Desen ve İşlemler

Deneysel Süreçten Önceki İşlemler	Yöntem	Deneysel Süreçten Sonraki İşlemler
Kişisel bilgi formunun uygulanması Ön-testin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması	Çevrimiçi Ortamda Eş Zamansız Eğitim Video konferans aracı ile eş zamanlı eğitim	Son-testin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması Açık uçlu bir anket formunun uygulanması Sistemin kapatılmasından dört hafta sonra kalıcılık testinin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması

Araştırmanın asıl uygulama süreci için deneysel desen ve süreç Tablo 2'de verilmiştir:

Tablo 2

Asıl Uygulama Süreci İçin Deneysel Desen ve Süreç

Deneysel Süreçten Önceki İşlemler	Çalışma Grubu	Yöntem	Deneysel Süreçten Sonraki İşlemler
Kişisel bilgi formunun uygulanması Ön-testin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması	Deney Grubu I	Çevrimiçi ortamda eş zamansız eğitim	Son-testin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması Açık uçlu anket formunun uygulanması Kalıcılık testinin(Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması
Kişisel bilgi formunun uygulanması Ön-testin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması	Deney Grubu II	Çevrimiçi ortamda eş zamansız eğitim Video konferans aracıyla eş zamanlı eğitim	Son-testin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması Açık uçlu anket formunun uygulanması Kalıcılık testinin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması

Çalışma Grubu

Araştırmanın çalışma grubunu; Ankara ilinde merkezi bir ortaokulda 6.sınıfta öğrenim görmekte olan ve Bilişim Teknolojileri ve Yazılım dersine katılan öğrenciler oluşturmuştur. Veri toplama süreci ve çevrimiçi ortama katılım süreci gönüllük esasına göre yürütülmüş olup, öğrencilerin velilerinden gerekli izinler çevrimiçi ortamda bir form aracılığıyla alınmıştır.

Çalışma Grubunun Özellikleri

Araştırmanın pilot uygulama ve asıl uygulama sürecine katılan çalışma gruplarının özellikleri ayrı başlıklar halinde sunulmuştur.

Katılımcılarla ilgili demografik bilgiler. Araştırmanın çalışma grubunu Ankara ilinde merkezi bir ortaokulda öğrenim görmekte olan 6. sınıf öğrencileri oluşturmaktadır. Katılımcıların profili; cinsiyet, interneti kullanım amaçlarına yönelik ayrılan süre vb. gibi farklı durumlar açısından çeşitlilik göstermektedir.

Pilot uygulamaya katılan çalışma grubu ile ilgili demografik bilgiler. Araştırmanın pilot uygulama sürecine aynı sınıfta eğitim görmekte olan 30 altıncı sınıf öğrencisi katılmıştır. Kişisel bilgi formu aracılığıyla elde edilen veriler alt başlıklar halinde sunulmuştur.

Katılımcıların cinsiyete göre dağılımları. Araştırmanın pilot çalışma grubunun %60'ını (f=18) kadın ve %40'ını (f=12) erkek olmak üzere 30 öğrenci oluşmaktadır (Bkz. Tablo 3).

Tablo 3

Katılımcıların Cinsiyete Göre Dağılımları

Cinsiyet	%	n
Kadın	60	18
Erkek	40	12
Toplam	100	30

Katılımcıların kendilerine ait bir bilgisayarı olma durumuna göre dağılımları. Araştırmanın pilot çalışma grubundaki öğrencilerin %40'ının (f=12) kendisine ait bir bilgisayarının olmadığı; %23,3'ünün (f=7) bir yıldır, %26,7'sinin (f=8) 2-5 yıldır, %10'unun (f=3) 6 yıl ve üzeri süreyle kendilerine ait bir bilgisayarının bulunduğu görülmüştür (Bkz. Tablo 4).

Tablo 4

Katılımcıların Kendilerine Ait Bir Bilgisayarı Olma Durumuna Göre Dağılımları

Kullanım Süresi	%	n
Sahip Değilim.	40	12
1 Yıl	23.3	7
2-5 Yıl	26.7	8
6 Yıl ve Üzeri	10	3
Toplam	100	30

Katılımcıların kendilerine ait bir akıllı telefona sahip olma durumuna göre dağılımları. Araştırmanın pilot çalışma grubundaki öğrencilerin %40'ının (f=12) kendisine ait bir akıllı telefona sahip olmadığı; %46,7'sinin (f=14) bir yıldır ve %13,3'ünün (f=4) 2-5 yıldır kendilerine ait bir akıllı telefona sahip olduğu görülmüştür (Bkz. Tablo 5).

Tablo 5

Katılımcıların Kendilerine Ait Bir Akıllı Telefona Sahip Olma Durumuna Göre Dağılımları

Kullanım Süresi	%	n
Sahip Değilim.	40	12
1 Yıl	46.7	14
2-5 Yıl	13.3	4
Toplam	100	30

Katılımcıların dizüstü bilgisayar (notebook, netbook, ultrabook vb.) kullanma sıklığına göre dağılımları. Araştırmanın pilot çalışma grubundaki öğrencilerin %16,7'sinin (f=5) bazen, %16,7'sinin (f=5) nadiren, %16,7'sinin (f=5) her zaman, %30'unun (f=9) ara sıra dizüstü bilgisayar kullandıkları, %20'sinin (f=6) ise hiçbir zaman dizüstü bilgisayar kullanmadıkları görülmüştür (Bkz.Tablo 6).

Tablo 6

Katılımcıların Dizüstü Bilgisayar (Notebook, netbook, ultrabook vb.) Kullanma Sıklığına Göre Dağılımları

Kullanım Sıklığı	%	n
Nadiren	16.66	5
Ara sıra	30	9
Bazen	16.66	5
Her zaman	16.66	5
Hiçbir zaman	20	6
Toplam	100	30

Katılımcıların tablet bilgisayar kullanma sıklığına göre dağılımları. Araştırmanın pilot çalışma grubundaki öğrencilerin %26,7'sinin (f=8) nadiren, %13,3'ünün (f=4) ara sıra, %10'unun (f=3) bazen, %16,7'sinin (f=5), her zaman tablet kullandıkları; %33,3'ünün (f=10) ise hiçbir zaman tablet bilgisayar kullanmadıkları görülmüştür (Bkz. Tablo 7).

Tablo 7

Katılımcıların Tablet Bilgisayar Kullanma Sıklığına Göre Dağılımları

Kullanım Sıklığı	%	n
Nadiren	26.7	8
Ara sıra	13.3	4
Bazen	10	3
Her Zaman	16.7	5
Hiçbir Zaman	33.3	10
Toplam	100	30

Katılımcıların akıllı telefon kullanma sıklığına göre dağılımları. Araştırmanın pilot çalışma grubundaki öğrencilerin %6,7'sinin (f=2) nadiren, %30'unun (f=9) ara sıra, %16,7'sinin (f=5) bazen, %33,3'ünün (f=10) her zaman akıllı telefon kullandıkları; %13,3'ünün (f=4) ise hiçbir zaman akıllı telefon kullanmadıkları görülmüştür (Bkz. Tablo 8).

Tablo 8

Katılımcıların Akıllı Telefon Kullanma Sıklığına Göre Dağılımları

Kullanım Sıklığı	%	n
Nadiren	6.7	2
Ara sıra	30	9
Bazen	16.7	5
Her Zaman	33.3	10
Hiçbir Zaman	13.3	4
Toplam	100	30

Katılımcıların bilgisayar/internet kullanımına ilişkin günlük ortalama ayırdıkları süreye göre dağılımları. Araştırmanın pilot çalışma grubundaki öğrencilerin %20'sinin (f=6) bir saatten az, %43,3'ünün (f=13) 1-3 saat, %30'unun (f=9) 4-6 saat, %6,7'sinin (f=2) 7 saat ve üzeri bilgisayar/İnternet kullanımına ilişkin günlük ortalama süre ayırdıkları görülmüştür (Bkz. Tablo 9).

Tablo 9

Katılımcıların Bilgisayar/İnternet Kullanımına İlişkin Günlük Ortalama Ayırdıkları Süreye Göre Dağılımları

Günlük Ortalama Ayrılan Süre	%	n
1 Saatten Az	20	6
1-3 saat	43.3	13
4-6 saat	30	9
7 saat ve üzeri	6.7	2
Toplam	100	30

Katılımcıların interneti haber okumak- medyayı takip etmek amaçlı günlük kullanım süresine göre dağılımları. Araştırmanın pilot çalışma grubundaki öğrencilerin %40'ının (f=12) 15 dakikadan az, %23,3'ünün (f=7) 1 saatten az, %6,7'sinin (f=2) 1-3 saat haber okumak- medyayı takip etmek amaçlı günlük internet kullanımlarının olduğu; %30'unun (f=9) ise hiçbir zaman interneti haber okumak-medyayı takip etmek amaçlı kullanmadıkları görülmüştür (Bkz. Tablo 10).

Tablo 10

Katılımcıların İnterneti Haber Okumak- Medyayı Takip Etmek Amaçlı Günlük Kullanım Süresine Göre Dağılımları

Günlük Ortalama Ayrılan Süre	%	n
15 Dk'dan Az	40	12
1 Saatten Az	23.3	7
1-3 saat	6.7	2
Hiçbir zaman	30	9
Toplam	100	30

Katılımcıların interneti eğlence amaçlı kullanım süresine göre dağılımları. Araştırmanın pilot çalışma grubundaki öğrencilerin %6,7'sinin (f=2) günlük 15 dakikadan az, %20'sinin (f=6) bir saatten az, %56,7'sinin (f=17) 1-3 saat, %13,3'ünün (f=4) 4-6 saat, %3,3'ünün (f=1) 7 saat ve üzeri interneti eğlence amaçlı kullanımlarının olduğu belirlenmiştir (Bkz. Tablo 11).

Tablo 11

Katılımcıların İnterneti Eğlence Amaçlı Kullanım Süresine Göre Dağılımları

Günlük Ortalama Ayrılan Süre	%	n
15 Dk'dan az	6.7	2
1 saatten az	20	6
1-3 saat	56.7	17
4-6 saat	13.3	4
7 saat ve üzeri	3.3	1
Toplam	100	30

Katılımcıların interneti eğitim amacıyla kullanım (araştırma yapmak, ödev yapmak, uzaktan eğitime devam etmek) süresine göre dağılımları. Araştırmanın pilot çalışma grubundaki öğrencilerden büyük çoğunluğunun (%76,7) interneti eğitim amacıyla kullanmak (araştırma yapmak, ödev yapmak, uzaktan eğitime devam etmek) için günlük 1-3 saat, %13,3'ünün (f=4) bir saatten az ve %10'unun (f=3) 4-6 saat zaman ayırdıkları görülmüştür (Bkz. Tablo 12).

Tablo 12

Katılımcıların İnterneti Eğitim Amacıyla Kullanım (Araştırma Yapmak, Ödev Yapmak, Uzaktan Eğitime Devam Etmek) Süresine Göre Dağılımları

Günlük Ortalama Ayrılan Süre	%	n
1 Saatten Az	13.3	4
1-3 saat	76.7	23
4-6 saat	10	3
Toplam	100	30

Kişisel bilgi formundan elde edilen veriler doğrultusunda, pilot uygulamanın çalışma grubunu oluşturan öğrencilerin grafiğinin cinsiyet, kendilerine ait bir bilgisayar vb. cihaza sahip olma durumu ve interneti kullanım amaçlarına yönelik ayrılan süre açısından dengeli bir dağılım gösterdiğini söylemek mümkündür.

Katılımcıların bilgi güvenliği hakkında daha önce herhangi bir eğitim alma durumuna göre dağılımları. Araştırmanın pilot çalışma grubundaki öğrencilerden büyük çoğunluğunun (%76,7) bilgi güvenliği hakkında daha önce herhangi bir eğitim almadığı; %23,3'ünün (f=7) ise eğitim aldığı tespit edilmiştir (Bkz. Tablo 13).

Tablo 13

Katılımcıların Bilgi Güvenliği Hakkında Daha Önce Herhangi Bir Eğitim Alma Durumuna Göre Dağılımları

Eğitim Alma Durumu	%	n
Evet	23.3.	7
Hayır	76.7	23
Toplam	100	30

Asıl uygulamaya katılan çalışma grubu ile ilgili demografik bilgiler. Araştırmanın asıl uygulama sürecine katılacak olan öğrenciler aynı okulda dört farklı sınıfta öğrenim görmekte olan 6.sınıf öğrencilerden gönüllülük esasına göre belirlenmiştir. Bu doğrultuda 52 öğrenci çalışmaya gönüllü olarak katılmak istediğini belirtmiştir. Dört ayrı şubenin ön-test puanlarına dayalı olarak normallik varsayımları sınanmış; sınıf mevcutları 50'den küçük olduğundan Shapiro-Wilks testine başvurulmuştur (Bkz. Tablo 14).

Tablo 14

Ön-Test Sonuçlarına İlişkin Shapiro-Wilks Normallik Testi Sonuçlarının Dağılımı

Sınıflar	Sd	p
Şube 1	8	0.03
Şube 2	11	0.02
Şube 3	18	0.75
Şube 4	15	0.08

Tablo 14 incelendiğinde; Şube 1 ve Şube 2'deki öğrencilerin ortalama puanlarının normal dağılımdan anlamlı (aşırı) sapma gösterdiği (p<.05); Şube 3 ve Şube 4'teki öğrencilerin ortalama puanlarının normal dağılımdan anlamlı (aşırı) sapma göstermediği (p>.05) görülmektedir. Bu sebeple, grupların ön-test puanlarının analizine yönelik parametrik olmayan istatistiksel yöntemlerden Kruskall Wallis H-Testinin kullanımına karar verilmiştir (Bkz. Tablo 15).

Tablo 15

Ön-Test Sonuçlarına İlişkin Kruskall Wallis H-Testi Sonuçlarının Dağılımı

Sınıflar	n	Sıra Ortalaması	ss	X^2	p	Anlamlı Fark
Şube 1	8	26,56	3	0.00	1.00	-
Şube 2	11	26,36				
Şube 3	18	26,69				
Şube 4	15	26,33				
Toplam	52					

Şubelerin ön-test puanlarına ilişin Kruskall Wallis H-Testi sonuçları, öğrencilerin çevrimiçi güvenlik ve risk ile ilgili düzeylerinin; şubeye bağlı olarak değişmediğini göstermektedir, x^2 (sd=3, n=52) = 0.00, *p*>.05. Dört farklı şubede yer alan öğrencilerin ön-test puan ortalamaları Tablo 16'da verilmiştir.

Tablo 16

Asıl Uygulama Sürecine Katılım Sağlayan Şubelerin Ön-Test Puan Ortalamaları

Sınıflar	N	N
Şube 1	8	71.75
Şube 2	11	69.27
Şube 3	18	76.44
Şube 4	15	74.93

Tablo 16'da görüldüğü üzere; Şube 3 ve Şube 4'te yer alan öğrencilerin ön-test puanları ortalaması, Şube 1 ve Şube 2'de yer alan öğrencilerin ön-test puanları ortalamasına göre istatistiksel anlamda farklı olmasa da biraz daha yüksek olarak belirlenmiştir. Deneysel uygulamanın iç geçerliliğini artırabilmek adına; Şube 1 ve Şube 3'ün Deney Grubu I; Şube 2 ve Şube 4'ün Deney Grubu II olarak atanmasına karar verilmiştir. Bu koşullar altında Deney Grubu I'de 26 ve Deney Grubu II'de 26 olmak üzere 52 altıncı sınıf öğrencisi ile çalışma yürütülmüştür. Öğrencilerden kişisel bilgi formu aracılığıyla elde edilen veriler alt başlıklar halinde sunulmuştur.

Katılımcıların interneti haber okumak- medyayı takip etmek amaçlı günlük kullanım sürelerine göre dağılımı. Araştırmanın asıl uygulama sürecine katılan öğrencilerin %38,46'sının (f=20)15 dakikadan az, %25'inin (f=13) 15 dakika -1saat, %15,38'inin (f=8) 1-3 saat, %1,92'sinin (f=1) 4 saat ve üzeri haber okumak-medyayı takip etmek amaçlı günlük internet kullanımlarının olduğu**;** %19,23'ünün (f=10) ise hiçbir zaman interneti haber okumak- medyayı takip etmek amaçlı kullanmadıkları görülmüştür (Bkz. Tablo 17).

Tablo 17

Katılımcıların İnterneti Haber Okumak- Medyayı Takip Etmek Amaçlı Günlük Kullanım Süresine Göre Dağılımları

Günlük Kullanım Süresi	%	n
Hiç kullanmıyorum.	19.23	10
15 dakikadan az.	38.46	20
15 dakika - 1saat.	25	13
1-3 saat.	15.38	8
4 saat ve üzeri.	1.92	1
Toplam	100	52

Katılımcıların interneti eğlence amaçlı günlük kullanım sürelerine göre dağılımı. Araştırmanın asıl uygulama sürecine katılan öğrencilerin %21,15'inin (f=11) 15 dakikadan az, %30,77'sinin (f=16) 15 dakika-1 saat, %38,46'sının (f=20) 1-3 saat, %9,61'inin (f=5) 4 saat ve üzeri eğlence amaçlı günlük internet kullanımlarının olduğu görülmüştür (Bkz. Tablo 18).

Tablo 18

Katılımcıların İnterneti Eğlence Amaçlı Kullanım Sürelerine Göre Dağılımları

Günlük Kullanım Süresi	%	n
Hiç kullanmıyorum.	0	-
15 dakikadan az.	21.15	11
15 dakika - 1saat.	30.77	16
1-3 saat.	38.46	20
4 saat ve üzeri.	9.61	5
Toplam	100	52

Katılımcıların interneti eğitim amaçlı günlük kullanım sürelerine göre dağılımı. Araştırmanın asıl uygulama sürecine katılan öğrencilerin %13.46'sının (f=7) 15 dakikadan az, %17.31'inin (f=9) 15 dakika-1saat, %28,84'ünün (f=15) 1-3 saat, %36,54'ünün (f=19) 4 saat ve üzeri eğitim amaçlı günlük internet kullanımlarının olduğu; %3,85'inin (f=2) ise hiçbir zaman interneti eğitim amaçlı kullanmadıkları görülmüştür (Bkz. Tablo 19).

Tablo 19

Katılımcıların İnterneti Eğitim Amaçlı Kullanım Sürelerine Göre Dağılımları

Günlük Kullanım Süresi	%	n
Hiç kullanmıyorum.	3.85	2
15 dakikadan az.	13.46	7
15 dakika - 1saat.	17.31	9
1-3 saat.	28.84	15
4 saat ve üzeri.	36.54	19
Toplam	100	52

Kişisel bilgi formu aracılığıyla elde edilen veriler doğrultusunda araştırmanın asıl uygulama sürecine katılan öğrencilerin grafiğinin interneti kullanım amaçlarına yönelik günlük ayırdıkları süre açısından dengeli bir dağılım gösterdiklerini söylemek mümkündür.

Katılımcıların bilgi güvenliği hakkında daha önce yüz yüze ortamda bir eğitim alma durumuna göre dağılımı. Araştırmanın asıl uygulama sürecine katılan öğrencilerin %86,54'sinin (f=45) bilgi güvenliği hakkında daha önce yüz yüze ortamda bir eğitime katıldığı ve %13,46'sının (f=7) yüz yüze ortamda birkaç eğitime katıldığı görülmüştür (Bkz. Tablo 20).

Tablo 20

Katılımcıların Bilgi Güvenliği Hakkında Daha Önce Yüz Yüze Ortamda Bir Eğitim Alma Durumuna Göre Dağılımları

Bilgi Güvenliği Hakkında Daha Önce Yüz Yüze Ortamda Bir Eğitim Alma Durumu	%	n
Yüz yüze bir eğitime katıldım.	86,54	45
Yüz yüze birkaç eğitime katıldım.	13.46	7
Toplam	100	52

Katılımcıların bilgi güvenliği hakkında daha önce çevrimiçi ortamda bir eğitim alma durumuna göre dağılımı. Araştırmanın asıl uygulama sürecine katılan öğrencilerin %69,2'si (f=36) bilgi güvenliği hakkında daha önce çevrimiçi ortamda hiç eğitim almamış, %19,2'si (f=10) çevrimiçi bir eğitime katılmış ve %11,5'i (f=6) çevrimiçi birkaç eğitime katılmış durumdadır. (Bkz. Tablo 21).

Tablo 21

Katılımcıların Bilgi Güvenliği Hakkında Daha Önce Çevrimiçi Ortamda Bir Eğitim Alma Durumuna Göre Dağılımları

Bilgi Güvenliği Hakkında Daha Önce Çevrimiçi Ortamda Bir Eğitim Alma Durumu	%	n
Hiç eğitim almadım.	69.2	36
Çevrimiçi bir eğitime katıldım.	19.2	10
Çevrimiçi birkaç eğitime katıldım.	11.5	6
Toplam	100	52

Araştırma Süreci

Araştırmanın deneysel uygulamaları için pilot çalışma 2020-2021 Eğitim-Öğretim yılı 1. yarıyılında gerçekleştirilmiştir. Pilot uygulama sürecine katılmış olan çalışma grubu, deneysel uygulamalara katılan çalışma grubundan farklı olarak belirlenmiştir. Pilot uygulama sürecinde, araştırmanın uygulanması sürecinde yaşanan sorunlar tespit edilmiş ve bu sorunların çözümüne yönelik işlemler yapılmıştır. 2020-2021 Eğitim-Öğretim yılı 2. yarıyılında araştırmanın asıl uygulaması yapılmıştır. Araştırmanın asıl uygulaması, kişisel bilgi formu ve ön-testin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması ile başlatılmış olup, son-test (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) ile sürdürülmüştür. Son olarak ise, öğrenmenin kalıcılığının sınanabilmesi amacıyla, eğitimler tamamlandıktan sonra çevrimiçi sistemdeki içerikler kalıcılığın belirlenmesine yönelik sonuçların daha güvenilir olması amacıyla erişime kapatılmış ve dört hafta sonra; daha önce uygulanmış olan sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı tekrar uygulanmıştır.

Pilot uygulama süreci. Araştırmanın pilot uygulama sürecinde yapılan işlemler Tablo 22'de gösterilmiştir.

Tablo 22

Pilot Uygulama Sürecinde Yapılan İşlemler

Haftalar	Etkinlikler
Hafta 1	Katılımcıların süreç hakkında bilgilendirilmesi, katılımcıların çevrimiçi ortamının incelemesi, kişisel bilgi formu ve ön-testin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması
Hafta 2-Hafta 5	Çevrimiçi ortamda öğrenme etkinlikleri ve eş zamanlı dersler
Hafta 6	Açık uçlu anket formu ve son-testin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması
Hafta 10	Öğrenmenin kalıcılığının sınanması amacıyla kalıcılık testinin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması

Çevrimiçi ortamdaki öğrenme etkinlikleri kapsamında her hafta öğrencilere birtakım görevler verilmiş ve öğrencilerin bu görevleri tamamlamaları için bir hafta süre tanınmıştır. Süreç içerisinde sistem üzerinden öğrencilerin etkinlikleri katılım durumları takip edilmiştir. Öğrencilerin görevleri tamamlamasının ardından o haftanın konularına yönelik olarak geliştirilen çevrimiçi ortamdan bağımsız bir video konferans aracıyla eş zamanlı ders gerçekleştirilmiştir. Öğrencilerin video konferans aracı ile yürütülen derslere yüksek oranda katılım sağladıkları, ders esnasında sorulan soruları cevaplama konusunda istekli davrandıkları gözlenmiştir. Eğitim tamamlandıktan sonra açık uçlu anket formu ile araştırmanın deneysel uygulamalarında ulaşılan nicel verileri destekleyecek nitel verilere ulaşılması planlanmıştır. Araştırmanın pilot uygulamaları, COVID-19 küresel salgın koşullarında yüz yüze eğitimin ve iletişimin mümkün olmadığı koşullarda gerçekleştirildiğinden yarı yapılandırılmış görüşme formu ile ulaşılması planlanan verilere, çevrimiçi ortamda açık uçlu anket formu ile ulaşılmak durumunda kalınmıştır. Tablo 23'te öğrencilerin haftalık olarak tamamladıkları konular yer almaktadır.

Tablo 23

Pilot Uygulama Sürecinde Öğrencilerin Haftalık Görevleri

Haftalar	Etkinlikler
Hafta 1	İnternetin Bilinçli Kullanımı Ünitesi - Kişisel Verilerin Korunması Konusu İnternetin Bilinçli Kullanımı Ünitesi - Sosyal Ağlar Konusu Bağımsız bir çevrimiçi ortamda eş zamanlı derse katılım
Hafta 2	İnternetin Bilinçli Kullanımı Ünitesi – Internet Okuryazarlığı Konusu İnternetin Bilinçli Kullanımı Ünitesi – Siber Zorbalık Konusu İnternetin Bilinçli Kullanımı Ünitesi – Çevrimiçi Riskler Konusu Ünite Sonu Etkinlikler Sayfası Bağımsız bir çevrimiçi ortamda eş zamanlı derse katılım
Hafta 3	Internet ve Ağ Güvenliği Ünitesi -Şifre Güvenliği Konusu Internet ve Ağ Güvenliği Ünitesi -Zararlı Yazılımlar Konusu Bağımsız bir çevrimiçi ortamda eş zamanlı derse katılım
Hafta 4	Internet ve Ağ Güvenliği Ünitesi -Web Güvenlik Önlemleri Konusu Internet ve Ağ Güvenliği Ünitesi -Güvenli Olmayan İletişim Yolları Konusu Ünite Sonu Etkinlikler Sayfası Bağımsız bir çevrimiçi ortamda eş zamanlı derse katılım

Pilot uygulama süreci için araştırmanın veri kaynaklarını, veri toplanması ve veri analizini içeren araştırma süreci Tablo 24'te sunulmuştur.

Tablo 24

Pilot Uygulama Süreci için Araştırmanın Ana Hatları

Araştırma Problemi	Veri Kaynağı	Verilerin Toplanması	Veri Analizi
Öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri nedir?	Çalışma Grubu Öğrencileri	Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı	Betimsel İstatistikler
Öğrencilerin bilgi güvenliği hakkında daha önce herhangi bir eğitim alma durumunun sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerine etkisi nedir?	Çalışma Grubu Öğrencileri	Kişisel Bilgi Formu Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı	Betimsel İstatistikler Bağımsız Gruplar t-testi Tek Yönlü ANOVA Testi
Sanal ortamlarda bilgi güvenliği eğitimine yönelik tasarlanan ortamda yürütülen eğitimlerin öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerine etkisi nedir?	Çalışma Grubu Öğrencileri	Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı	Bağımlı Gruplar t-testi
Sanal ortamlarda bilgi güvenliği eğitimine yönelik tasarlanan ortamda yürütülen eğitimlerin öğrenilenlerin kalıcılığına etkisi nedir?	Çalışma Grubu Öğrencileri	Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı	Bağımlı Gruplar t-testi
"Öğrencilerin sanal ortamlarda bilgi güvenliğine yönelik geliştirilen çevrimiçi ortam hakkındaki görüşleri nelerdir?"	Çalışma Grubu Öğrencileri	Açık uçlu anket formu	Betimsel İstatistikler

Pilot uygulama ön-test (sanal ortamlara bilgi güvenliğine ilişkin düzeyi belirleme aracı) kodlayıcı uyum analizleri. Araştırmacı tarafından geliştirilmiş olan sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracının güvenilirliğini belirleyebilmek amacıyla uygulanan ön-test iki ayrı kodlayıcı tarafından kodlanmış, her soru için Kappa istatistiği kullanılarak kodlayıcı uyum değerleri hesaplanmıştır. Soruların kodlanması sürecinde kullanılacak puanlama ölçütleri ölçme aracının geliştirilmesi sürecinde uzmanlarca (10 bilişim teknolojileri öğretmeni) değerlendirilmiştir (EK-5). Ölçme aracında yer alan soruların Kappa değerlerinin yorumlanabilmesi amacıyla ise Landis ve Koch (1977)'nin önerdiği tablo dikkate alınmıştır (Bkz. Tablo 25).

Tablo 25

Kappa İstatistiği Değeri ve Uyum Yorumu

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

Kaynak: Landis, J. R. ve Koch, G. G. (1977) "The measurement of observer agreement for categorical data" ,*Biometrics*. Cilt. 33, say. 159-174

Kappa istatistiği kullanılarak hesaplanan kodlayıcı uyum değerleri Tablo 26'da sunulmuştur:

Tablo 26

Ön-teste Yönelik Kappa İstatistiği Sonuçlarının Dağılımı

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

Tablo 26'da görüldüğü üzere; ölçme aracında yer alan 3., 4., 5., 6., 7., 8., 9 ila 10. ve 11. soruların uyum düzeyi güçlü; 1. ve 2. soruların uyum düzeyi ise mükemmeldir. Bu veriler doğrultusunda ölçme aracının iki ayrı kodlayıcı puanlaması açısından güvenilir olduğu söylenebilir.

Araştırmanın pilot uygulama sürecine yönelik bulgular. Araştırma kapsamında geliştirilen ortamın kullanılabilirlik sorunlarının belirlenmesi, sistemde düzenlemeler yapılabilmesi ve eğitimin etkililiğinin sınanabilmesi amacıyla asıl uygulamadan önce pilot uygulama gerçekleştirilmiştir. Araştırmanın pilot uygulama süreci Ankara ilinde merkezi bir ortaokulda öğrenim görmekte olan altıncı sınıf öğrencileriyle çevrimiçi ortamda yürütülmüştür. Pilot uygulama sürecinde veri toplama aracı olarak; kişisel bilgi formu, ön-test, son-test ve kalıcılık testi (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) ile açık uçlu anket formuna başvurulmuştur. Veri toplama araçlarından elde edilen bulgular alt başlıklar halinde sunulmuştur.

Öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerine yönelik bulgular. Pilot uygulama sürecinin ilk araştırma sorusu "Öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri nedir?" şeklindedir. Öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerini belirleyebilmek amacıyla ön-test uygulanmış, ön-testi 30 altıncı sınıf öğrencisi cevaplamıştır. Pilot çalışma grubu öğrencilerinin ön-testten almış oldukları puanlar Ek 9'da sunulmuştur. Ön-test sonuçları incelendiğinde; öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin iyi bir seviyede olduğu görülmüş, ancak bilgi güvenliği ile ilgili olarak planlanmış kapsamlı bir eğitimin öğrencilerin bilgi düzeylerine ve farkındalıklarına daha fazla katkı sağlayacağı düşünülmüştür.

Kişisel bilgi formu aracılığıyla; öğrencilerin bilgi güvenliği hakkında daha önce bir eğitim alma durumuna yönelik veriler toplanmıştır. Öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin ölçülmesi için ise araştırmacı tarafından geliştirilen sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracına başvurulmuştur.

Verilerin analizi sürecinde bilgisayar tabanlı bir istatistik programından faydalanılmıştır. Öğrencilerin kişisel bilgilerinin belirlenmesinde betimsel analizlerden faydalanılmıştır. Pilot çalışma grubunun ön-test sonuçları sanal

ortamlarda bilgi güvenliğine ilişkin düzeyleri açısından değerlendirmeye alınmıştır. Pilot çalışma grubunun sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri için verilerin normal dağılım gösterip göstermediğini belirlemek amacıyla Shapiro-Wilks testi kullanılmış ve analiz sonucu $p>.05$ olduğundan; grubun normal dağılım gösterdiğine karar verilmiştir.

Öğrencilerin bilgi güvenliği hakkında daha önce herhangi bir eğitim alma durumunun sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerine etkisi. Pilot uygulama sürecinin ikinci araştırma sorusu "Öğrencilerin bilgi güvenliği hakkında daha önce herhangi bir eğitim alma durumunun öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerine etkisi nedir?" şeklindedir. Öğrencilerin bilgi güvenliği hakkında daha önce herhangi bir eğitim alma durumunun sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri açısından etkisinin belirlenmesi amacıyla bağımsız grup t-test analizine başvurulmuştur. Bu analizin sonuçları Tablo 27'de verilmiştir.

Tablo 27

Öğrencilerin Bilgi Güvenliği Hakkında Daha Önce Herhangi Bir Eğitim Alma Durumu ve Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeylerine Göre Bağımsız Gruplar t-testi Sonuçları

Eğitim Alma Durumu	N	X	S	sd	t	p
Evet	7	62.85	27.05	28	.30	.76
Hayır	23	65.26	15.27		.22	

Tablo 27'de görüldüğü üzere, öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri; bilgi güvenliği hakkında daha önce herhangi bir eğitim alma durumuna göre değişmemektedir, $t(28)=.30$, $p>.05$.

Sanal ortamlarda bilgi güvenliği eğitimine yönelik tasarlanan ortamda yürütülen eğitimlerin öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerine etkisi. Pilot uygulama sürecinin üçüncü araştırma sorusu "Sanal ortamlarda bilgi güvenliği eğitimine yönelik tasarlanan ortamda yürütülen eğitimlerin öğrencilerin sanal ortamlarda bilgi güvenliğine öğrenmelerine etkisi nedir?" şeklindedir. Bu araştırma sorusu doğrultusunda uygulanan ön-testten alınan puanlar EK-H'de ve son-testten alınan puanlar EK-I'da verilmiştir. Pilot çalışma grubunun sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri için verilerin normal

dağılım gösterip göstermediğini belirlemek amacıyla ön-test ve son-test verilerine yönelik uygulanan Shapiro-Wilks testinin sonuçları Tablo 28'de verilmiştir.

Tablo 28

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

Uygulanan Test	Sd	P
Ön test	30	0.18
Son-test	30	0.23

Tablo 28'de görüldüğü üzere, ön-test ve son-test sonuçlarına yönelik uygulanan Shapiro-Wilks testi analiz sonuçlarına göre α>05 olduğundan; pilot çalışmaya katılan grubun normal dağılım gösterdiğine karar verilmiştir. Bu doğrultuda katılımcıların sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri üzerindeki etkililiğinin test edilmesi için parametrik istatistik yöntemlerinden bağımlı gruplar t-testinin uygulanmasına karar verilmiştir. Çalışma grubunun ön-test ve son-test sonuçlarının karşılaştırılmasına ilişkin bağımlı gruplar t-testi sonuçları Tablo 29'da verilmiştir.

Tablo 29

Çalışma Grubunun Ön-test ve Son-test Sonuçlarının Karşılaştırılmasına İlişkin Bağımlı Gruplar t-testi Sonuçları

Test	N	X	S	sd	t	p
Ön-test	30	64.70	18.15	29	-8.50	0.000
Son-test	30	91.80	14.92			

Tablo 29'da görüldüğü üzere, çevrimiçi ortamda yapılan eğitimler sonrasında öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinde anlamlı bir artış olduğu belirlenmiştir, $t(29)=-8.50$, $p<.05$. Öğrencilerin eğitim öncesi sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri puanları ortalaması X= 64,70 iken, eğitim sonrasında sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri ortalaması X= 91,80'e yükselmiştir. Bu bulgu, çevrimiçi ortamda yürütülen bilgi güvenliği eğitimlerinin, öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin artırılmasında önemli bir etkisinin olduğu şeklinde yorumlanabilir.

Sanal ortamlarda bilgi güvenliği eğitimine yönelik tasarlanan ortamda yürütülen eğitimlerin öğrenilenlerin kalıcılığına etkisi. Pilot uygulama sürecinin dördüncü araştırma sorusu "Sanal ortamlarda bilgi güvenliği eğitimine yönelik tasarlanan ortamda yürütülen eğitimlerin öğrenilenlerin kalıcılığına etkisi nedir?" şeklindedir. Bu araştırma sorusu doğrultusunda uygulanan kalıcılık testinden alınan puanlar EK-İ'de verilmiştir. Pilot çalışma grubunun sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri için verilerin normal dağılım gösterip göstermediğini belirlemek amacıyla kalıcılık testi verilerine yönelik uygulanan Shapiro-Wilks testi sonuçları Tablo 30' da verilmiştir.

Tablo 30

Kalıcılık Testi Sonuçlarına İlişkin Shapiro-Wilks Normallik Testi Sonuçlarının Dağılımı

Uygulanan Test	Sd	P
Kalıcılık Testi	30	0.38

Tablo 30'da görüldüğü üzere kalıcılık testi sonuçlarına yönelik uygulanan Shapiro-Wilks testi analiz sonuçlarına göre $p>.05$ olduğundan; pilot çalışmaya katılan grubun kalıcılık testi bağlamında normal dağılım gösterdiğine karar verilmiştir. Bu doğrultuda, parametrik istatistiksel yöntemlerden bağımlı gruplar t-testinin kullanılmasının uygun olduğuna karar verilmiştir. Araştırma kapsamında yürütülen deneysel uygulamanın öğrenilenlerin kalıcılığı açısından değerlendirilebilmesi amacıyla çalışma grubunun son-test ve kalıcılık testi sonuçlarının karşılaştırılmasına ilişkin bağımlı gruplar t-testi sonuçları Tablo 31'de verilmiştir.

Tablo 31

Çalışma Grubunun Son-test ve Kalıcılık Testi Sonuçlarının Karşılaştırılmasına İlişkin Bağımlı Gruplar t-testi Sonuçlarının Dağılımı

Test	N	X	S	sd	t	P
Son-Test	30	91.80	14.92	29	2.10	0.040
Kalıcılık Testi	30	87.26	14.26			

Tablo 31'de görüldüğü üzere pilot çalışma sonucunda eğitimlerin tamamlanmasından dört hafta sonra son-test tekrar uygulanmış ve eğitimin kalıcılık açısından değerlendirilmesi yapılmıştır. Son-test ve kalıcılık testi verileri

karşılaştırıldığında, öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri açısından anlamlı farklılık olmadığı belirlenmiştir, $t(29)=2.10$, $p>.05$. Öğrencilerin son-testten almış oldukları sanal ortamlarda bilgi güvenliğine ilişkin düzey puanları ortalaması X= 91,80 iken, eğitim tamamlandıktan dört hafta sonra yapılan kalıcılık testinde sanal ortamlarda bilgi güvenliğine ilişkin düzey puanları ortalaması X= 87,26 olarak belirlenmiştir. Bu bulgu, çevrimiçi ortamda yürütülen eğitimler tamamlandıktan dört hafta sonra yapılan değerlendirmenin, öğrenilenlerin kalıcılığı açısından olumlu olduğu şeklinde yorumlanabilir.

Açık uçlu anket formu bulguları. Pilot uygulama sürecinin beşinci ve son araştırma sorusu "Öğrencilerin sanal ortamlarda bilgi güvenliğine yönelik geliştirilen çevrimiçi ortam hakkındaki görüşleri nelerdir?" şeklindedir. Bu araştırma sorusu doğrultusunda uygulanan açık uçlu anket formunu 30 altıncı sınıf öğrencisi doldurmuştur. Açık uçlu anket formu aracılığıyla elde edilen veriler alt başlıklar halinde sunulmuştur:

Sitenin isminin uygunluğuna yönelik bulgular. Öğrencilerin tamamı (30) sitenin isminin uygun olduğunu belirtmiştir.

Sitede bulunan içeriklerin güncelliğine yönelik bulgular. Öğrencilerin tamamı (30) sitede bulunan içeriklerin güncel olduğunu belirtmiştir.

Video ve anlatıların süresinin ne kadar olması (daha uzun-kısa) gerektiğine yönelik bulgular. Açık uçlu anket formu aracılığıyla öğrencilerin; ortamda yer alan video ve anlatıların süresinin ne kadar olması (Daha Uzun-Kısa) gerektiğine yönelik görüşleri toplanmıştır. Ortamda bilgi güvenliği ile ilgili videoların süresine ilişkin; 12 öğrenci, video sürelerinin ideal olduğunu; yedi öğrenci daha kısa olması gerektiğini, altı öğrenci daha uzun olması gerektiğini; beş öğrenci ise video sürelerinin konunun içeriğine göre değişmesi gerektiğini belirtmiştir.

"Kendimizi Sınayalım" bölümleri hakkındaki görüşlere yönelik bulgular. Açık uçlu anket formu aracılığıyla öğrencilerin **"**Kendimizi Sınayalım" bölümleri hakkındaki görüşlerine yönelik veri toplanmıştır. 25 öğrenci "kendimizi sınayalım" bölümlerinin, konuları pekiştirmelerine yardımcı olduğunu, örneklerle daha iyi kavradıklarını, neler öğrenip öğrenmediklerini fark etmelerini sağladığını, bu bölümlü etkili ve keyifli bulduklarını belirtmişlerdir. Beş öğrenci ise, soru sayısının az olduğunu belirtmiştir.

“Etkinlikler” başlıklı bölümde yer alan etkinlikler hakkındaki görüşlere yönelik bulgular. Açık uçlu anket formu aracılığıyla öğrencilerin “Etkinlikler” başlıklı bölümde yer alan etkinlikler hakkındaki görüşlerine yönelik veri toplanmıştır. 26 öğrenci “Etkinlikler” bölümündeki bütün etkinliklerin ilgisini çektiğini, dört öğrenci etkinlikleri mobil teknolojiler aracılığıyla yaparken sorun yaşadıklarını, iki öğrenci etkinliklerin ilgisini çekmediğini, iki öğrenci bazı etkinliklerin ilgisini çektiğini, bir öğrenci ise sadece “Örnek Durum Çözümleme” etkinliğini beğenmediğini belirtmiştir.

Ortamın en çok hangi yönünün beğenildiğine yönelik bulgular. Açık uçlu anket formu aracılığıyla öğrencilerin ortamın en çok hangi yönünü beğendiklerine yönelik veri toplanmıştır. Sekiz öğrenci oyunlar bölümünü, sekiz öğrenci içeriklerin faydalı olmasını, eğitici, açık ve anlaşılır olmasını, altı öğrenci etkinlikleri, altı öğrenci keyifli ve eğlenceli olmasını, dört öğrenci videoları, iki öğrenci soru sor kısmını, iki öğrenci ortamdaki bütün bölümleri beğendiklerini, bir öğrenci arkadaşlar bölümünü beğendiğini, bir diğer öğrenci ise ortamı öğretmeni oluşturduğu için ortamın ilgisini çektiğini belirtmiştir

Ortamın en az hangi yönünün beğenildiğine yönelik bulgular. Açık uçlu anket formu aracılığıyla öğrencilerin ortamın en az hangi yönünü beğendiğine yönelik veri toplanmıştır. 11 öğrenci ortamda beğenmediği bir yön olmadığını, dört öğrenci oyunlarda zaman zaman hata oluştuğunu, iki öğrenci yapmış oldukları etkinliklerin yapılıp yapılmadığının görünmediğini, iki öğrenci metinlerin uzun olduğunu belirtmiştir. 11 öğrencinin ortamda beğenmedikleri yönlere ilişkin cümleler şu şekildedir:

“Etkinlikler bölümündeki bulmaca kafa karıştırıcı” (Öğrenci 9)

“Kelime bulmacada yazılar zor yazılıyor” (Öğrenci 22)

“Etkinliklerin telefondan yapılmamasını beğenmedim” (Öğrenci 20)

“Etkinlikleri beğenmedim” (Öğrenci 24)

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

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

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

“Videolar YouTube dan alındığı için tam ekran yapılmaması” (Öğrenci 25)

“Videoları beğenmedim” (Öğrenci 2)

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

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

Ortamın bilgi güvenliği hakkında sağladığı katkılar. Açık uçlu anket formu aracılığıyla ortamın bilgi güvenliği hakkında sağladığı katkılara yönelik veri toplanmıştır. 13 öğrenci bilmedikleri konuları öğrendiklerini; 13 öğrenci internette daha dikkatli, bilinçli ve tedbirli davranması gerektiğini öğrendiklerini belirtmiştir. Dört öğrencinin ortamın çevrimiçi güvenlik ve risk hakkında ne gibi katkılar sağladığına ilişkin cümleleri ise şu şekildedir:

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

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

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

“Şifrelerimi düzgün belirlemeye başladım.” (Öğrenci 15)

Ortamın kullanıldığı süreçte karşılaşılan zorluklar. Açık uçlu anket formu aracılığıyla öğrencilerin ortamı kullandıkları süreçte karşılaştıkları zorluklara yönelik veri toplanmıştır. 14 öğrenci ortamı kullandıkları süreçte herhangi bir zorlukla karşılaşmadıklarını, üç öğrenci etkinlikleri telefondan yapamadıklarını, iki öğrenci video kısmında reklamların çıkabildiğini, iki öğrenci tamamladıkları bölümlerin bazen kaydedilmediğini ve iki öğrenci oyunlar kısmında oyunların zaman zaman takıldığını belirtmişlerdir. Yedi öğrencinin ortamı kullandıkları süreçte karşılaştıkları zorluklara ilişkin görüşleri ise şu şekildedir:

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

“Bazen videoları açmakta zorlanıyorum.” (Öğrenci 14)

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

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

“Etkinliklerdeki bulmaca kısmında zorlandım.” (Öğrenci 15)

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

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

Öğrencilere yönelik sanal ortamlarda bilgi güvenliği eğitiminde başka hangi konulara yer verilmesi gerektiğine yönelik bulgular. Açık uçlu anket formu aracılığıyla öğrencilere yönelik bir sanal ortamlarda bilgi güvenliği eğitiminde başka hangi konulara yer verilmesi gerektiğine yönelik veri toplanmıştır. 10 öğrenci, web sitesindeki konuların yeterli olduğunu ve yedi öğrenci farklı konu önerisi hakkında fikrinin olmadığını belirtmiştir. Bir öğrenci ise bilgi güvenliği eğitimiyle ilgisi olmayan bir konu önerisinde bulunmuştur.12 öğrencinin, öğrencilere yönelik bir eğitimde başka hangi konulara yer verilmesi gerektiğine ilişkin ifadeleri aşağıdaki şekildedir:

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

“Bu konularda daha fazla ne yapabiliriz, kendimizi sanal ortamda nasıl sınırlamayı öğrenmeliyiz, vb.” (Öğrenci 10)

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

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

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

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

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

“Her ünitede ayrı bölümlere yer verilmeli.” (Öğrenci 28)

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

“Bulmaca eklenmeli.” (Öğrenci 13)

“Kelime türetmece eklenmeli.” (Öğrenci 14)

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

Ortamda yer alan “yeni yorum ekle” bölümünde diğer kullanıcılarla gerçekleştirilen iletişimin sağladığı katkılar. Açık uçlu anket formu aracılığıyla ortamda yer alan “yeni yorum ekle” bölümünde diğer kullanıcılarla gerçekleştirilen iletişimin öğrencilere sağladığı katkılara yönelik veri toplanmıştır. 21 öğrenci, diğer arkadaşlarıyla fikir alışverişi yapmalarını sağladığını, farklı bilgiler öğrendiklerini,

sekiz öğrenci, yorum ekle bölümünü kullanmadıklarını ve çok gerekli bulmadıklarını, bir öğrenci ise bilgilerini pekiştirmesini sağladığını belirtmiştir.

Ortama yönelik öneriler. Açık uçlu anket formu aracılığıyla öğrencilere ortama yönelik öneriler sorulmuştur. 23 öğrenci ortama yönelik bir önerisinin olmadığını belirtmiştir. Yedi öğrencinin ortama yönelik önerileri ise aşağıdaki şekildedir:

> *"Videolar biraz daha yavaş olabilir, hızlı geçen yazıları okumak için durdurmak zorunda kalıyorsun." (Öğrenci 8)*
>
> *"Daha farklı etkinlik bulmaca boşluk doldurma, Doğru-Yanlış soruları eklenebilir." (Öğrenci 9)*
>
> *"Telefondaki hatalar düzeltilmeli. Yani telefondan da rahat bir şekilde yapılmalı." (Öğrenci 16)*
>
> *"İçinde olduğumuz ve olacağımız güvenlik tehlikeleri sık sık tekrarlanmalı bence." (Öğrenci 10)*
>
> *"'Devamı' yazısının daha büyük olması ve daha fazla oyun, etkinlik olması." (Öğrenci 29)*
>
> *"Hackerlardan nasıl korunmamız gerektiğini öğreten bir konu."(Öğrenci 25)*
>
> *"Etkinlikler bölümüne doğru/yanlış eklenebilir." Öğrenci 22*

Pilot uygulama süreci sonunda öğrencilerin sanal ortamlarda bilgi güvenliğine yönelik geliştirilen çevrimiçi ortam hakkındaki görüşleri dikkate alınarak çevrimiçi ortamda yapılan değişiklikler şu şekildedir:

Uzun metinlerin yer aldığı sayfalarda metinlerin kısaltılması,

Web tarayıcılarına yönelik güvenlik önlemleri hakkında açıklamalar eklenmesi,

Videoların sistemin içerisine dâhil edilmesi, tam ekran yapılamama ve reklam sorununun giderilmesi,

Etkinliklerin mobil uygulamalarda kullanımı sırasında çıkan sorunların giderilmesi,

"Kendimizi Sınayalım" bölümlerinde yer alan soru sayısının artırılması

Asıl uygulama süreci. Pilot uygulama sürecinde elde edilen verilerden yola çıkarak; çevrimiçi ortam içerikleri ve tasarımında düzenlemeler gerçekleştirildikten sonra araştırmanın asıl uygulama süreci başlatılmıştır. Araştırmanın asıl uygulama sürecinde yapılan iş ve işlemler Tablo 32'de gösterilmiştir.

Tablo 32

Çalışma Grubunun Dahil Olduğu Veri Toplama Süreci

Haftalar	Etkinlikler
Hafta 1	Katılımcıların süreç hakkında bilgilendirilmesi, katılımcıların çevrimiçi ortamı incelemesi, kişisel bilgi formu ve ön-testin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması,
Hafta 2-Hafta 5	Çevrimiçi ortamda öğrenme
Hafta 6	Açık uçlu anket formu ve son-testin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması
Hafta 10	Kalıcılık testinin (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) uygulanması

Pilot uygulama sürecinde yapılan iş ve işlemler asıl uygulama sürecinde de gerçekleştirilmiştir. Bu kapsamda yine, çevrimiçi ortamdaki öğrenme etkinlikleri kapsamında her hafta öğrencilere birtakım görevler verilmiş ve öğrencilerin bu görevleri tamamlamaları için bir hafta süre tanınmıştır. Süreç içerisinde sistem üzerinden öğrencilerin etkinliklere katılım durumları takip edilmiş, velilere gerekli bilgilendirmeler yapılmıştır. Deney Grubu I öğrencileri; çevrimiçi ortamdaki eğitimleri eş zamansız olarak takip etmişlerdir. Deney Grubu II öğrencileri ise, çevrimiçi ortamdaki eğitimleri eş zamansız takip etmenin yanı sıra, her hafta öğretmenin video konferans aracı ile yürüttüğü eş zamanlı derslere katılmışlardır. Deney grubu II öğrencilerinin eş zamanlı derslere katılım düzeyleri Tablo 33'te yer almaktadır.

Tablo 33

Asıl Uygulama Sürecinde Deney grubu II Öğrencilerinin Eş Zamanlı Derslere Katılım Oranı

Haftalar	Deney Grubu II Öğrenci Sayısı	Eşzamanlı Derse Katılan Öğrenci Sayısı	%
Hafta 1	26	20	79,92
Hafta 2	26	18	69,23
Hafta 3	26	18	69,23
Hafta 4	26	17	65,38

Tablo 33'te görüldüğü üzere eş zamanlı derslere katılım, her hafta Deney Grubu II'de, grup mevcudunun yarısından fazla olmakla beraber, hiçbir zaman bütün öğrencilerin eş zamanlı derse katılımı sağlanamamıştır. Bu duruma yönelik bazı öğrencilerin velileri, bulundukları yerlerdeki birtakım aksaklıklar (internetin veya bilgisayarın olmaması) sebebiyle öğrencilerin derse katılamadıklarını bildirmişlerdir.

Birkaç öğrenci ise dersleri takip edememe sebebi olarak, katılmış oldukları diğer zorunlu çevrimiçi derslere yönelik ödevlerinin fazla olmasını göstermişlerdir.

Eğitimler tamamlandıktan sonra açık uçlu anket formu ile araştırmanın deneysel uygulamalarında ulaşılan nicel verileri destekleyecek nitel verilere ulaşılması planlanmıştır. Araştırmanın asıl uygulamaları, COVID-19 küresel salgın koşullarında yüz yüze eğitimin ve iletişimin mümkün olmadığı koşullarda gerçekleştirildiğinden; yarı yapılandırılmış görüşme formu ile ulaşılması planlanan verilere, çevrimiçi ortamda açık uçlu anket formu ile ulaşılmak durumunda kalınmıştır. Tablo 34'te öğrencilerin her hafta tamamladıkları konular yer almaktadır.

Tablo 34

Asıl Uygulama Sürecinde Öğrencilerin Haftalık Görevleri

Gruplar	Haftalar	Etkinlikler
Deney Grubu I	Hafta 1	İnternetin Bilinçli Kullanımı Ünitesi - Kişisel Verilerin Korunması Konusu İnternetin Bilinçli Kullanımı Ünitesi - Sosyal Ağlar Konusu
Deney Grubu I	Hafta 2	İnternetin Bilinçli Kullanımı Ünitesi – Internet Okuryazarlığı Konusu İnternetin Bilinçli Kullanımı Ünitesi – Siber Zorbalık Konusu İnternetin Bilinçli Kullanımı Ünitesi – Çevrimiçi Riskler Konusu Ünite Sonu Etkinlikler Sayfası
Deney Grubu I	Hafta 3	Internet ve Ağ Güvenliği Ünitesi -Şifre Güvenliği Konusu Internet ve Ağ Güvenliği Ünitesi -Zararlı Yazılımlar Konusu
Deney Grubu I	Hafta 4	Internet ve Ağ Güvenliği Ünitesi -Web Güvenlik Önlemleri Konusu Internet ve Ağ Güvenliği Ünitesi -Güvenli Olmayan İletişim Yolları Konusu Ünite Sonu Etkinlikler Sayfası
Deney Grubu II	Hafta 1	İnternetin Bilinçli Kullanımı Ünitesi - Kişisel Verilerin Korunması Konusu İnternetin Bilinçli Kullanımı Ünitesi - Sosyal Ağlar Konusu Bağımsız bir çevrimiçi ortamda eş zamanlı derse katılım
Deney Grubu II	Hafta 2	İnternetin Bilinçli Kullanımı Ünitesi – Internet Okuryazarlığı Konusu İnternetin Bilinçli Kullanımı Ünitesi – Siber Zorbalık Konusu İnternetin Bilinçli Kullanımı Ünitesi – Çevrimiçi Riskler Konusu Ünite Sonu Etkinlikler Sayfası Bağımsız bir çevrimiçi ortamda eş zamanlı derse katılım
Deney Grubu II	Hafta 3	Internet ve Ağ Güvenliği Ünitesi -Şifre Güvenliği Konusu Internet ve Ağ Güvenliği Ünitesi -Zararlı Yazılımlar Konusu Bağımsız bir çevrimiçi ortamda eş zamanlı derse katılım
Deney Grubu II	Hafta 4	Internet ve Ağ Güvenliği Ünitesi -Web Güvenlik Önlemleri Konusu Internet ve Ağ Güvenliği Ünitesi -Güvenli Olmayan İletişim Yolları Konusu Ünite Sonu Etkinlikler Sayfası Bağımsız bir çevrimiçi ortamda eş zamanlı derse katılım

Asıl uygulama süreci için araştırmanın veri kaynakları, veri toplanması ve veri analizini içeren araştırma süreci Tablo 35'te sunulmuştur:

Tablo 35

Asıl Uygulama Süreci için Araştırmanın Ana Hatları

Araştırma Alt Problemleri	Veri Kaynağı	Verilerin Toplanması	Veri Analizi
Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri nedir?	Deney Grubu I Deney Grubu II	Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeyi Belirleme Aracı	Betimsel İstatistikler
Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri, bilgi güvenliği hakkında daha önce yüz yüze ortamda bir eğitim alma durumuna göre nasıl değişmektedir?	Deney Grubu I Deney Grubu II	Kişisel Bilgi Formu Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeyi Belirleme Aracı	Betimsel İstatistikler Bağımsız Gruplar t-testi Mann Whitney U-Testi
Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri, bilgi güvenliği hakkında daha önce çevrimiçi ortamda bir eğitim alma durumuna göre nasıl değişmektedir?	Deney Grubu I Deney Grubu II	Kişisel Bilgi Formu Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeyi Belirleme Aracı	Betimsel İstatistikler Tek Faktörlü ANOVA Kruskal Wallis H-Testi
Sanal ortamlarda bilgi güvenliği ile ilgili eğitime yönelik tasarlanan ortamda yürütülen eğitimlerin ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliği ile ilgili bilgi durumlarındaki değişimlerine etkisi nedir?	Deney Grubu I Deney Grubu II	Kişisel Bilgi Formu Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeyi Belirleme Aracı	Bağımlı Gruplar t-testi Wilcoxon İşaretli Sıralar Testi
Çevrimiçi ortamda yürütülen bilgi güvenliği ile ilgili eğitimlerin öğrenilenlerin kalıcılığına etkisi nedir?	Deney Grubu I Deney Grubu II	Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeyi Belirleme Aracı	Bağımlı Gruplar t-testi Wilcoxon İşaretli Sıralar Testi
Çevrimiçi ortamda eş zamansız eğitimlere katılan ortaokul öğrencileri ile eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliğine yönelik öğrenmeleri açısından istatistiksel olarak anlamlı bir fark var mıdır?	Deney Grubu I Deney Grubu II	Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeyi Belirleme Aracı	Bağımsız Gruplar t-testi

Çevrimiçi ortamda eş zamansız eğitimlere katılan öğrenciler ile eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliğine yönelik öğrenilenlerin kalıcılığı açısından istatistiksel olarak anlamlı bir fark var mıdır?	Deney Grubu I Deney Grubu II	Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeyi Belirleme Aracı	Mann Whitney U-Testi
Sanal ortamlarda bilgi güvenliği ile ilgili olarak çevrimiçi ortamda yürütülen eğitimlere katılan öğrencilerin aldıkları eğitime yönelik görüşleri nelerdir?	Deney Grubu I Deney Grubu II	Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeyi Belirleme Aracı	İçerik analizi ve betimsel analiz

Asıl uygulama süreci ön-test (sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) kodlayıcı uyum analizleri. Araştırmacı tarafından geliştirilmiş olan sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracının güvenilirliği pilot çalışma kapsamında belirlenmiş olmakla birlikte, farklı bir çalışma grubu ile farklı zamanlarda ölçme aracının tekrar kullanılması sebebiyle güvenilirliğin tekrar sınanmasının anlamlı olacağı düşünülmüştür. Bu bağlamda güvenilirliği belirleyebilmek amacıyla ön-test iki ayrı kodlayıcı tarafından kodlanmış, Kappa istatistiği kullanılarak kodlayıcı uyum değerleri 0,73 olarak hesaplanmıştır. Ölçme aracında yer alan soruların Kappa değerlerinin yorumlanabilmesi amacıyla Landis ve Koch (1977)'nin önerdiği tablo dikkate alınmıştır (Bkz. Tablo 25). Bu veriler doğrultusunda ölçme aracının iki ayrı kodlayıcı puanlaması açısından güvenilir olduğu söylenebilir.

Asıl uygulama süreci son-test (sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) kodlayıcı uyum analizleri. Araştırmacı tarafından geliştirilmiş olan sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracının güvenilirliğini belirleyebilmek amacıyla son-test iki ayrı kodlayıcı tarafından kodlanmış, Kappa istatistiği kullanılarak kodlayıcı uyum değerleri 0,70 olarak hesaplanmıştır. Ölçme aracında yer alan soruların Kappa değerlerinin yorumlanabilmesi amacıyla Landis ve Koch (1977)'nin önerdiği tablo dikkate alınmıştır (Bkz. Tablo 25). Bu veriler doğrultusunda ölçme aracının iki ayrı kodlayıcı puanlaması açısından güvenilir olduğu söylenebilir.

Asıl uygulama süreci kalıcılık testi (sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) kodlayıcı uyum analizleri. Araştırmacı tarafından geliştirilmiş olan sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracının güvenilirliğini belirleyebilmek amacıyla kalıcılık testi iki ayrı kodlayıcı tarafından

kodlanmış, Kappa istatistiği kullanılarak kodlayıcı uyum değerleri 0,77 olarak hesaplanmıştır. Ölçme aracında yer alan soruların kappa değerlerinin yorumlanabilmesi amacıyla Landis ve Koch (1977)'nin önerdiği tablo dikkate alınmıştır (Bkz. Tablo 25). Bu veriler doğrultusunda ölçme aracının iki ayrı kodlayıcı puanlaması açısından güvenilir olduğu söylenebilir.

Araştırmacının rolü. Eğitimler; geliştirilen çevrimiçi ortamda yürütülmüş olup, öğrencilerin derslere katılım durumları araştırmacı tarafından takip edilmiş, velilere gerekli bilgilendirmeler araştırmacı tarafından yapılmıştır. Eş zamanlı dersler araştırmacı tarafından yürütülmüştür. Öğrenciler tarafından yanıtlanan ön test, son test, kalıcılık testi ve açık uçlu anketin değerlendirilmesi araştırmacı ve farklı bir kodlayıcı tarafından yapılmıştır.

İç ve dış geçerlik. Bağımlı değişkende gözlenen değişmelerin bağımsız değişkenle açıklanabilirlik derecesi iç geçerlik olarak tanımlanmaktadır (Büyüköztürk vd., 2020). Bu tez kapsamında iç geçerliliğe yönelik alınan önlemler şu şekildedir:

- Araştırmada ön test – son test statik grup deneysel desenine başvurulmuştur.
- Araştırmanın asıl uygulama sürecinde dört ayrı grup için gönüllülük esasına göre katılımcılar belirlenmiştir. Bütün grupların ön test bilgi düzeyi açısından denkliği belirlenmiştir. Bu doğrultuda katılımcı sayısının yeterli düzeyde olabilmesi amacıyla dört denk gruptan rastgele seçimle iki grup belirlenmiştir. Yine gruplar rastgele seçimle Deney I ve Deney II olmak üzere iki grup olarak atanmıştır. Ayrıca öğrencilerin daha önce çevrimiçi güvenlik ve risk ile ilgili bir eğitim alıp almadıkları belirlenerek, grupların denk olduklarına dair bir kanıt daha sağlanmaya çalışılmıştır.
- Öğrencilerin çevrimiçi güvenlik ve risk ile ilgili daha önce bir eğitim alma durumlarının; ön teste bağlı olarak çevrimiçi güvenlik ve risk ile ilgili bilgi düzeyleri açısından bir farklılık oluşturmadığı belirlenmiştir.
- Okullarda yüz yüze eğitimin yürütüldüğü olağan koşullarda gruplar arası etkileşimi sınırlandırmak pek mümkün olmamaktadır. Bu tez çalışmasının tamamen çevrimiçi ortamda yürütülmesi ve COVID-19 salgın sürecinde

gruplar arası etkileşimin okullardaki kadar fazla olmaması deneysel çalışmanın iç geçerliliği açısından bir avantaj sağlamıştır.

- İki farklı deney grubunun aynı eğitim içeriklerine aynı şartlar altında ve aynı süre tanınarak ulaşması sağlanmıştır.
- Araştırmacı yanlılığını engellemek amacıyla, çalışmada toplanan veriler farklı bir alan uzmanı tarafından da değerlendirilmiş ve kodlayıcı uyum değerleri raporlanmıştır.

Çevrimiçi Öğrenme Ortamının Geliştirilmesi

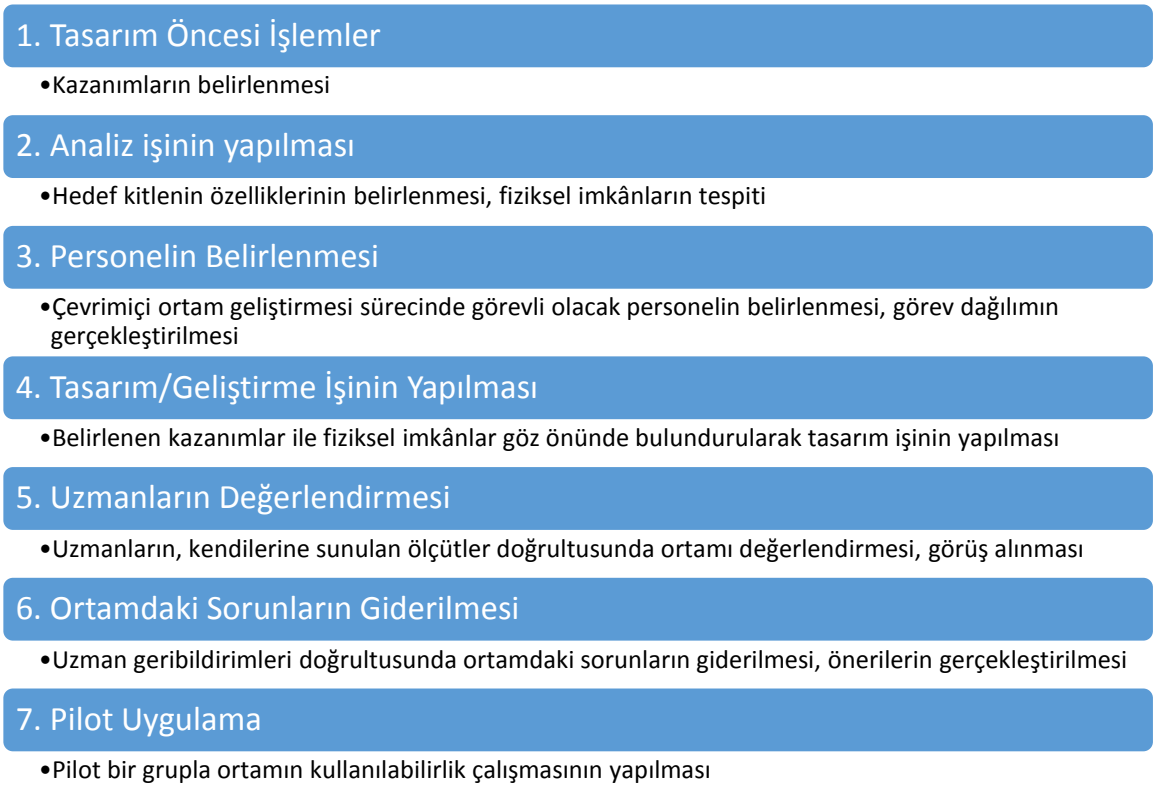
Çevrimiçi öğrenme ortamının geliştirilmesi sürecine ayrıntılı bir alanyazın taraması yapılarak başlanmıştır. Bu süreçte öncelikle etkili bir çevrimiçi öğrenme ortamının sahip olması gereken özellikler belirlenmiştir. Tüzün (2001) yerleşik bir dersin web-tabanlı uzaktan eğitim için yeniden tasarımına yönelik bir tasarım önerisi geliştirmiştir. Bu tasarım önerisi 9 aşamadan oluşmaktadır (Bkz. Tablo 36):

Tablo 36

Tüzün'ün 9 Aşamalı Web Tabanlı Ders Tasarımı Önerisi

	Tasarım Aşaması	Yürütülen İşlemler
1	Tasarım Öncesi Çabalar	Kazanımların belirlenmesi
2	Ders geliştirilmesi için bir merkezin oluşturulması	Çevrimiçi ortam tasarımının gerçekleştirileceği ortamın kararlaştırılması
3	Analiz işinin yapılması	Hedef kitlenin özelliklerinin belirlenmesi, fiziksel imkânların tespiti
4	Öğretim yöntemlerinin/stratejilerinin belirlenmesi	Kazanımlar doğrultusunda çevrimiçi ortamda kullanılacak yöntem ve stratejilerin belirlenmesi
5	Yönetsel yapının sağlanması	Çevrimiçi ortam geliştirmesi sürecinde görevli olacak personelin belirlenmesi
6	Tasarım/Geliştirme işinin yapılması	Belirlenen kazanımlar, yöntem ve teknikler ile fiziksel imkânlar göz önünde bulundurularak tasarım işinin yapılması
7	Dersin uygulanmasından önce teknolojik engellerin giderilmesi	Pilot bir grupla kullanılabilirlik çalışmasının yapılması
8	Öğrencilerin değerlendirilmesi	Çevrimiçi eğitim sonrasında öğrencilere son-testlerin uygulanması
9	Dersin değerlendirilmesi	Öğrencilerle yarı yapılandırılmış görüşmeler gerçekleştirilmesi

Çevrimiçi öğrenme ortamlarının tasarım sürecine yönelik alanyazında farklı tasarım önerileri yer almakla birlikte (Power, 2009; Balcı, 2010); Tüzün'ün (2001) 9 aşamalı tasarım önerisine benzer bir model çalışmada kullanılacak ortam için hazırlanmıştır (Bkz. Şekil 3):



Şekil 3. Çevrimiçi öğrenme ortamının tasarım sürecine yönelik model

Araştırmanın çalışma grubunu oluşturan öğrenciler beşinci sınıf düzeyinde, "Bilişim Teknolojileri ve Yazılım" dersi kapsamında sanal ortamlarda bilgi güvenliği ile ilgili olarak birtakım kazanımlara (Gizlilik ve Güvenlik; Doğru Bilgiye Erişim) yönelik eğitimler almışlardır (MEB Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı, 2018). Bu doğrultuda MEB Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı kapsamında öğrencilerin 5. sınıf ve 6.sınıf düzeyinde sanal ortamlarda bilgi güvenliği ile ilgili olarak edinmesi planlanan kazanımlar şu şekildedir (Bkz. Tablo 37):

Tablo 37

MEB Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı Sanal Ortamlarda Bilgi Güvenliğine Yönelik Kazanımları

Sınıf Düzeyi	Kazanımlar
5. Sınıf	• Bilişim teknolojileri ile İnterneti kullanma ve yönetme sürecinde etik ilkelere uymanın önemini açıklar. • Çevrimiçi ortamda başkalarının haklarına saygı duyar. • Dijital kimliklerin gerçeği yansıtmayabileceğini fark eder. • Dijital paylaşımların kalıcı olduğunu ve kendisinden geride izler bıraktığını fark eder. • Gizlilik açısından önemli olan bileşenleri belirler. • Gizli kalması gereken bilgi ile paylaşılabilecek bilgiyi ayırt eder.
6. Sınıf	• İnternet etiğinin önemini ifade eder. • Etik ilkelerin ihlali sonucunda karşılaşılabilecek durumlara örnekler verir. • Siber zorbalık kavramını açıklayarak korunma amacıyla alınabilecek önlemleri tartışır. • Telif hakkı kavramını ve önemini araştırır. • Bilişim suçlarının neler olduğunu açıklayarak ilgili kanunları özetler. • Bilişim suçlarına karşı alınabilecek önlemler ve stratejiler geliştirir. • Dijital paylaşımların kendisi ve başkaları üzerindeki etkilerini fark eder. • Bilişsel ve ahlaki gelişimine uygun olan dijital oyun ve içerikleri ayırt eder. • Bilişim teknolojilerinin kullanımında gizlilik ve güvenlik boyutlarının önemini tartışır. • Güvenlik açıklarının oluşumu konusunda yorum yapar. • Bilgi koruma yöntemlerini ifade eder. • Bilgi paylaşımı sürecinde olası riskleri değerlendirerek alınabilecek önlemleri tartışır. • Zararlı yazılımları kavrar. • Güvenlik yazılımlarının kullanım amaçlarını açıklar. • Bilgiye ulaşırken zararlı ve gereksiz içerikleri ayırt eder.

Çevrimiçi öğrenme ortamının geliştirilmesi sürecinde gerçekleştirilen alanyazın taraması, MEB Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı (2018) ve uzman görüşleri (Bilgisayar ve öğretim teknolojileri anabilim dalında doktorasını tamamlamış ve bilgi güvenliğine yönelik çalışmaları olan akademisyenler) dikkate alınarak ortamda yer alması planlanan kazanımlar ve ilgili konu başlıkları kararlaştırılmıştır. Bu doğrultuda çevrimiçi ortamda yer alan konu başlıkları ve ilgili kazanımlar Tablo 38'de verilmiştir:

Tablo 38

Çevrimiçi Öğrenme Ortamında Sanal Ortamlarda Bilgi Güvenliğine Yönelik Konu Başlıkları ve Hedeflenen Kazanımlar

Ünite	Konu	Hedeflenen Kazanımlar
1.Ünite: İnternetin Bilinçli Kullanımı	Kişisel Verilerin Korunması	• Kişisel verinin ne anlama geldiğini bilir. • Veri sorumlusunun kim olduğunu, veri sorumlusunun görev ve sorumluluklarını bilir. • Kişisel verileri koruma kurumu ve kişisel verileri koruma kanunu hakkında bilgi edinir. • Kişisel verileri korumaya yönelik ne gibi önlemler alabileceğini öğrenir.
1.Ünite: İnternetin Bilinçli Kullanımı	Sosyal Ağlar ve Mobil Ağlar	• Sosyal ağlarda paylaşılmaması gereken bilgilerin farkına varır. • Sosyal ağlarda dikkat edilmesi gereken hususlar hakkında bilgi edinir. • Mobil ağlarda dikkat edilmesi gereken hususlar hakkında bilgi edinir.
1.Ünite: İnternetin Bilinçli Kullanımı	İnternet Okuryazarlığı	• İnternette etkili arama yöntemlerini bilir. • İnternet bilgi ağlarında yer alan bilgilerin doğrulunu sorgular. • İnternette doğru bilgiye ulaşma yollarını bilir.
1.Ünite: İnternetin Bilinçli Kullanımı	Siber Zorbalık	• Siber zorba ve siber mağdur kavramları hakkında bilgi edinir. • Hangi Eylemlerin Siber Zorbalık Kapsamına girdiğini bilir. • Siber zorbalıktan korunma yollarını bilir. • Siber zorbalığa maruz kaldığında ne yapacağın bilir.
2.Ünite: İnternet ve Ağ Güvenliği	Şifre Güvenliği	• Güçlü şifre oluşturma yöntemlerini bilir.
2.Ünite: İnternet ve Ağ Güvenliği	Zararlı Yazılımlar	• Bilgisayar virüsleri, truva atları, solucanlar, casus yazılımlar hakkında bilgi edinir. • Bilgisayar virüsleri, truva atları, solucanlar, casus yazılımların çalışma prensibini bilir. • Bilgisayar virüsleri, truva atları, solucanlar, casus yazılımlardan korunma yollarını bilir.
2.Ünite: İnternet ve Ağ Güvenliği	Web Tarayıcılarına Yönelik Güvenlik Önerileri	• Web güvenliğiyle ilgili olarak tarayıcıları kullanırken alınabilecek güvenlik önlemlerini bilir.
2.Ünite: İnternet ve Ağ Güvenliği	Güvenli Olmayan İletişim Yolları	• İnternette genelde kullanılan ve bilgi alışverişini sağlayan erişim protokolleri hakkında bilgi edinir. • Web sayfalarındaki güvenli iletişim yolu kullanımını anlayabilir.

Ortam tasarımı ve geliştirme sürecinden sonra, ortamdaki sorunların belirlenmesi ve giderilmesi amacıyla, sekiz alan uzmanından (Bilgisayar ve öğretim teknolojileri anabilim dalında doktorasını tamamlamış ve ortam tasarımına yönelik çalışmaları olan akademisyenler) belirlenen ölçütler doğrultusunda görüş alınmıştır. Uzmanlardan gelen geribildirimlerdeki öneriler raporlanmış, ortamda iyileştirmeler yapılmıştır. Ortamın değerlendirilmesinde dikkate alınacak ölçütlerin belirlenebilmesi amacıyla bir alanyazın taraması yapılmıştır. Bu kapsamda Eren ve Erdem'in (2020); çocukları çevrimiçi güvenlik ve önlemler konusunda bilinçlendirmeye yönelik oluşturulan çevrimiçi ortamların nasıl olması gerektiği ile ilgili ve var olan sitelerin bu özellikler bağlamındaki durumunu ortaya koymak amacıyla bir çalışma gerçekleştirdiği tespit edilmiştir. Çalışma kapsamında, çocuklara kendilerini koruma becerisi kazandırmaya dönük çevrimiçi çoklu ortam ölçeği oluşturulmuştur. Çocuklara çevrimiçi ortamda koruma bilinci ve becerisi kazandırmak amacı ile hazırlanan 20 web sitesi belirlenmiş ve ölçeğin her bir maddesi her web sitesi için teker teker incelenmiştir. Çalışma sonuçlarına göre; incelenen sitelerin ölçeğin erişim ve motivasyon boyutlarını büyük oranda karşıladığı; ancak öğrenme, içerik ve aktif destek sistemi boyutlarının ise zayıf oranda karşılandığı belirlenmiştir.

Bu çalışma kapsamında; çevrimiçi ortamın tasarımı sürecinde, benzer içeriklere sahip web sitelerinin incelemesi yapılmıştır. Bu amaç doğrultusunda incelenen sitelerin adresleri aşağıdaki şekildedir:

1. Güvenli Çocuk : http://www.guvenlicocuk.org.tr/
2. Güvenli Web: https://www.guvenliweb.org.tr/
3. Güvenli İnternet: https://www.guvenlinet.org.tr/
4. eSafetykids: https://www.esafety.gov.au/kids
5. My safety net: https://mysafetynet.org.uk/
6. NetSmartzKids: https://www.netsmartzkids.org/
7. Thinkuknow: https://www.thinkuknow.co.uk/
8. internetmatters: https://www.internetmatters.org/

İncelenen sitelerdeki özellikler de dikkate alınarak kazanımların belirlenmesi, tasarım/geliştirme işinin yapılması aşamalarına yönelik çalışmalar yapılmıştır (Bkz. Şekil 3). Çevrimiçi ortam tasarımı sürecinde ortamın sahip olması gereken özelliklerin belirlenmesi amacıyla ise; Eren ve Erdem'in (2020) geliştirdiği ölçek maddeleri ölçüt olarak kabul edilmiştir (Bkz. Tablo 39):

Tablo 39

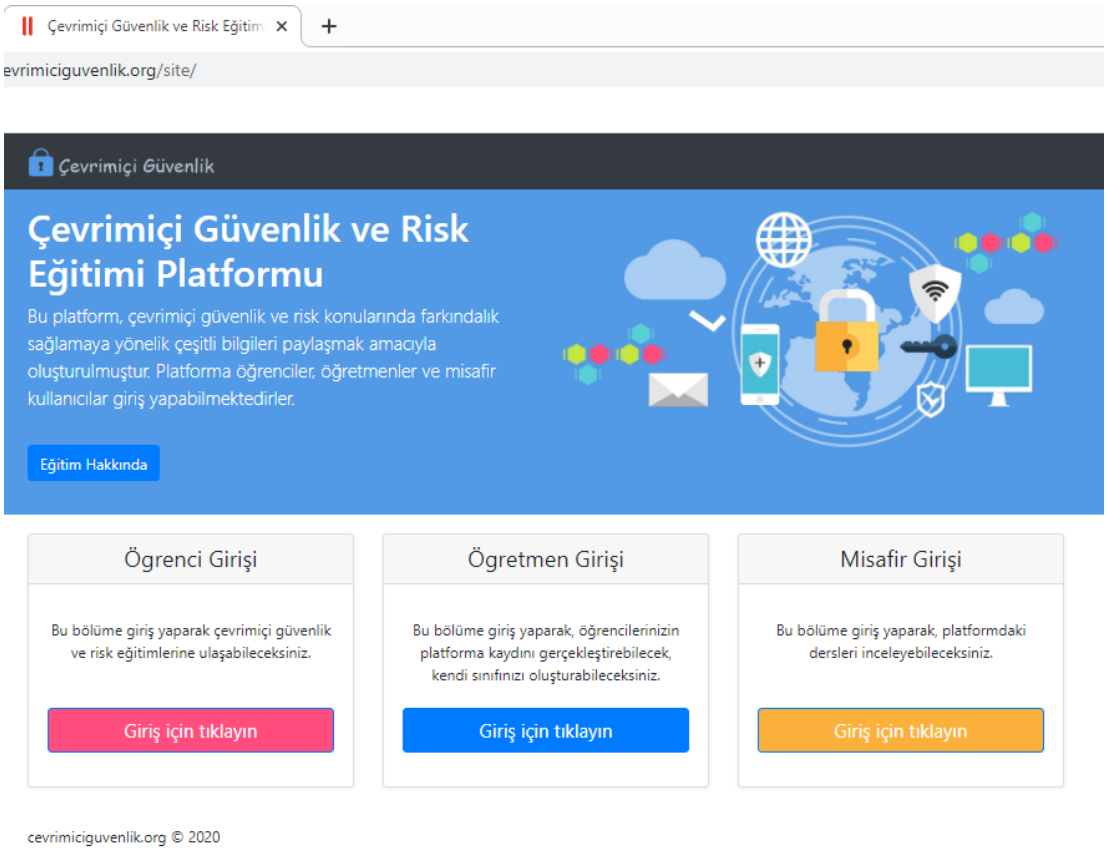
Çocuğa Kendini Koruma Becerisi Kazandırmaya Dönük Çevrimiçi Çoklu Ortam Ölçeği- Ölçek Boyutları ve Maddeleri

Boyutlar	Maddeler
Erişim Boyutu	1. Sitenin kolay hatırlanabilir, kısa bir adresi olmalıdır. 2. Sitedeki bilgi ve sayfalara kolaylıkla ulaşmayı sağlayacak bir etiketleme kullanılmalıdır. 3. Üye girişi olmadan kullanıcılara sitenin amacını, kapsamını ve potansiyel özelliklerini görebilme fırsatı verilmelidir. 4. Sitede, var olan belgelerin bilgisayara kaydedilmesi ya da ortama belge yüklenmesi kolay (belirgin bir yükleme simgesi) ve güvenli (virüs taraması) olmalıdır.
Motivasyon Boyutu	1. Sitede çocukların kendilerine ait profil sayfaları olmalıdır. 2. Profil sayfalarında çocuklar istedikleri kişilere profillerini açma seçeneğine sahip olmalıdırlar. 3. Ortam kullanıcılarının kendi ürünlerini saklama, paylaşma ve yazdırmalarına olanak vermelidir. 4. Üyelik girişi ile ortamın kullanıcıyı ya da kullanıcıların birbirlerini tanımaları, paylaşımda bulunmaları sağlanmalıdır. 5. Görsel tasarımda uyaran, parlak, canlı renkler kullanılarak tasarımın dikkat çekiciliği artırılmalıdır. 6. Ekranın düzenlenmesinde yalınlığa özen gösterilmeli, görsel karışıklıktan kaçınılmalıdır. 7. Dil kullanımında çocuksu vurgu ve tonlamalardan kaçınılmalıdır. 8. Ortam, eğlenceli, merak uyandırıcı nesneler, sorular, yazılar, videolarla zenginleştirilmelidir. 9. Video gibi nesnelerin yüklenme sürecinin izlenmesini sağlayacak bir mekanizma oluşturulmalıdır. 10. Animasyonların işlevinden bağımsız sürekli hareketliliğinden kaçınılmalıdır. 11. Çocuğun tamamlama duygusu hissetmesi ve oyuna bağımlı kalmaması için kısa ya da alt bölümlere ayrılmış oyunlar kullanılmalıdır. 12. Etkinlikler tamamlandığında animasyon izleme, sözcük oyunlar vs ve sonuçların gösterilmesi gibi ödüller verilmelidir. 13. Ortamdaki karakterler ses konuşma dil ve davranış gibi özellikler açısından tutarlılık göstermelidir. 14. İçerik ve etkinliklerde güncel olaylar konu edilmelidir. 15. Kullanıcıların içeriğe kendi ürünlerinin katkısı ile geliştirmelerine olanak sağlanmalıdır (yazı ve resim yarışmaları, kendi hikâyeleri, mektupları ile…).
Öğrenme boyutu	1. Profil sayfaları, adlandırma, avatar yaratma vb. özelleştirmelere olanak sağlayacak yapıda olmalıdır. 2. Anlatılarda konuşma diline yakın, etkileşimli bir dil kullanılmalıdır. 3. Metinler çocuğun söz varlığını dikkate alarak düzenlenmelidir. 4. Metinler kısa ve kurallı cümlelerden oluşmalıdır. 5. Metinler kısa bloklar halinde ve görsellerle desteklenerek sunulmalıdır. 6. Sesli anlatıların içeriği metnin içeriğini kapsayıcı olmalıdır. 7. Öğrenme süreci oyunlarla desteklenmelidir. 8. Oyunlar, ortamın amaç ve içeriği ile ilişkili olmalıdır. 9. Seçimin çocukta olduğu farklı etkileşim ve zorluk derecelerine sahip oyunlar kullanılmalıdır. 10. Çocuğa öğrenme etkinliklerini seçme fırsatı vermek için etkinlikler çeşitlendirilmelidir. 11. Ortam, çocukların diğer çocuklarla görüşlerini ilgi alanlarına göre paylaşabilecekleri eposta, forum, sohbet odaları gibi araçlar barındırmalıdır.

	12. Çocuğa hikâyeyi değiştirebileceği ya da aktivitenin içeriğini değiştirebileceği etkileşimli içerikler sunulmalıdır.
İçerik boyutu	1. İçerik yaşanmış ya da gerçeğe yakın biçimde kurgulanmış örnekler içermelidir. 2. Önemli kavramlar; risk durumlarını ve bunların olası nedenlerini içeren örneklere/problemlere gömülü olarak verilmelidir. 3. Farklı bakış açıları kazandırmak için aynı konudaki farklı örnekler birlikte sunulmalıdır. 4. Ele alınan örnekler/problemler belirli bir sonuçla bitmemiş, çoklu yorumlara açık olmalıdır. 5. Problemler/örnekler; nedenleri, sonuçları, tarafları vb. açılardan çok yönlü ele alınmalıdır. 6. İçerikteki problemlerde/ örneklerde duygusal boyutu öne çıkarmada aşırılıktan kaçınılmalıdır. 7. İçerik risk durumlarında yapılması gerekenler üzerine odaklanan örnekler içermelidir. 8. Kendi haklarına sahip çıkmanın ve diğerlerinin haklarına saygı duymanın, sorumluluklarını ve görevlerini yerine getirmenin önemini vurgulayan mesajlar verilmelidir. 9. Çocuğun kendini koruması gereken durumları diğer durumlardan ayırabilmesi için gerekli ipuçları verilmelidir. 10. Çocuklara güvendiği ve onlara destek olabilecek (yardım alabileceği) kişilerle durumlarını paylaşma, destek alma yönünde mesajlar verilmelidir.
Aktif Destek Sistemi boyutu	1. Çocuğun her türlü paylaşımı ya da sorusu için ekiple iletişime geçebileceği çevrimiçi iletişim olanakları (sohbet odası, msn…) sağlanmalıdır. 2. Sitede çocukların merak ettiği konuları sorabileceği, tartışabileceği uzman destekli ortamlar bulunmalıdır. 3. Çocuğa uygunsuz yorum, resim gibi içeriklerle karşılaştığında şikâyetini belirtebileceği bir sistem sağlanmalıdır. 4. Önemli, acil telefon numaraları, e-posta adresleri, ilgili kurum adresleri ortamda kolay erişilebilecek biçimde verilmelidir. 5. Çocuklara ortamda kendileri hakkında çok fazla kişisel bilgi vermelerinden kaynaklanabilecek riskler hatırlatılmalıdır.

Çevrimiçi öğrenme ortamı hakkında. Çevrimiçi öğrenme ortamı; ana sayfa giriş ekranı, eğitim modülleri ve alt modüller, eğitim hakkında, yardım, hesabım ve diğer içeriklere doğrudan erişimin sağlanabilmesi için ilgili bağlantıları içeren bir yapıda tasarlanmıştır. Aşağıda çevrimiçi ortamın bileşenleri ayrıntılı olarak sunulmuştur.

Ana sayfa giriş ekranı. Ana sayfa giriş ekranında çevrimiçi güvenlik ve risk ile ilgili eğitim platformuna ve eğitim hakkında açıklamalara yer verilmiştir. Ana sayfa giriş ekranına ait ekran görüntüsü Şekil 4'te görülmektedir:



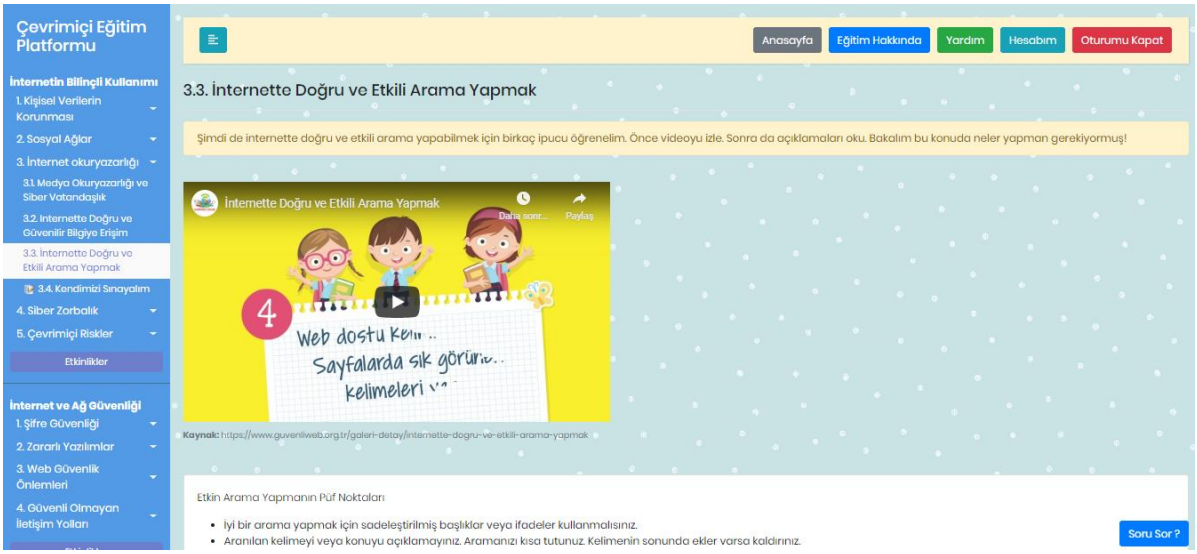
Şekil 4. Ana sayfa giriş ekranına ait ekran görüntüsü

Şekil 4'te görüldüğü üzere, ana sayfa giriş ekranında öğrenci, öğretmen ve misafir girişi olmak üzere üç ayrı kullanıcı girişi yer almaktadır. Sistem, öğretmenin öğrencisinin yapmış olduğu etkinlikleri izleyebileceği bir yapıda tasarlanmıştır.

Misafir girişi ile giriş yapıldığında, eğitim modülleri, kendimizi sınayalım, etkinlikler ve oyun içeriklerinin tamamına erişim sağlanabilmekte ancak, yapılan etkinlikler kayıt altına alınmamaktadır. Yine, misafir kullanıcı, "yorum yap" modülünü kullanabilmekte, ancak "öğretmene sor" modülünü herhangi bir sınıfa kayıtlı olmadığı için kullanamamaktadır.

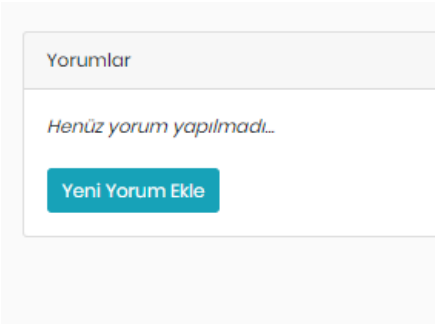
Eğitim modülleri. Bu bölümde kursun ana ve alt modülleri yer almaktadır. Modül içeriklerine erişim konusunda herhangi bir zaman kısıtlaması yoktur. Öğrencilerin öğrenme sürecinde zaman planlaması konusunda özgür olmaları sağlanmaktadır. Öğrenciler, öğrenme istekleri ve ihtiyaçları doğrultusunda öğrenme süreçlerini kendilerinin yönlendirebileceği konusunda bilgilendirilmiştir. Eğitim modülleri; ders amaçlarına uygun materyallerin sunulması, kendimizi sınayalım

bölümü, etkinlikler ve oyun olmak üzere 4 ana bileşenden oluşmaktadır (Bkz. Şekil 5)



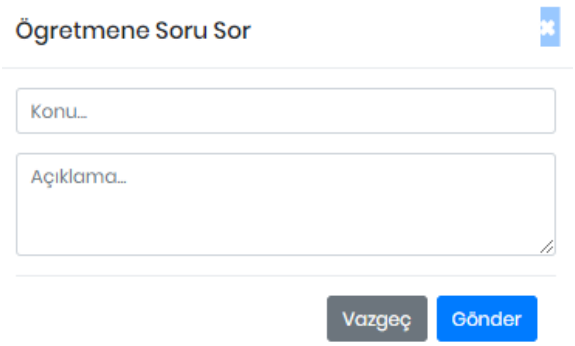
Şekil 5. Eğitim modülleri ekranına ait ekran görüntüsü

Her bileşen için öğrenciler sayfanın alt tarafında yer alan “Yeni Yorum Ekle” bölümünü kullanarak bölümler hakkında fikirlerini paylaşabilmektedirler (Bkz. Şekil 6).



Şekil 6.“Yeni Yorum Ekle” ekranına ait ekran görüntüsü

Öğrencilerin ortamı kullanırken öğretmenlerine kolayca erişebilmeleri ve danışabilmeleri için her sayfada sağ at köşeye “Soru sor” bileşeni yerleştirilmiştir (Bkz. Şekil 7).

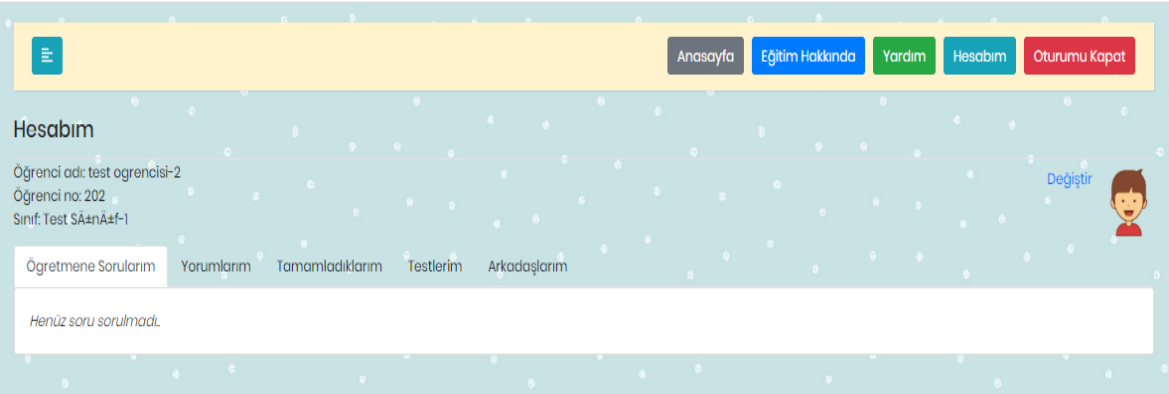


Şekil 7. “Soru Sor” ekranına ait ekran görüntüsü

Eğitim hakkında. Çevrimiçi öğrenme ortamının bu bileşeninde eğitim hakkında genel bilgilere yer verilmiştir. Bu bölümde; eğitim platformunun, geliştirilme amacından bahsedilmiş; çevrimiçi ortamlarda karşılaşılan güvenlik risklerini ve bu risklere yönelik alınabilecek önlemleri öğrencilerle paylaşmanın amaçlandığı açıklanmıştır. Yine bu bölümde, ortamın geliştirme süresinde görev alan araştırmacılar hakkında bilgi verilmiştir. Eğitim ve araştırmacılar hakkında verilen bilgiler doğrultusunda öğrencilerin güvenli ve motive bir şekilde sisteme katılım sağlaması amaçlanmıştır.

Yardım. Bu bölümde sıkça sorulan sorular aracılığıyla öğrencilerin faydalanabileceği bilgiler paylaşılmış olup, öğrencilerin “Öğretmene Sor” bileşeni ile destek alabileceğine yönelik açıklama yapılmıştır.

Hesabım. Bu bölümde öğrenci adı ve öğrenci numarası bilgileri yer almaktadır. Öğrencinin daha önce yapmış olduğu işlemleri görebilmesi amacıyla “hesabım” sayfası; “öğretmene sorularım, yorumlarım, tamamladıklarım ve testlerim olmak üzere dört bileşenden oluşmaktadır (Bkz. Şekil 8). Öğrencinin kendisini sisteme daha fazla ait hissedebilmesi için ise profil resmi değiştirme seçeneği yerleştirilmiştir.



Şekil 8. "Hesabım" sayfasına ait ekran görüntüsü

Veri Toplama Süreci

Araştırma sürecinde deneysel işlemin öncesinde ve sonrasında veri toplama işlemi gerçekleştirilmiştir. Bu bölümde, araştırma sürecinde kullanılan veri toplama araçları açıklanmıştır.

Veri Toplama Araçları

Bu çalışma kapsamında veri toplamak amacıyla; kişisel bilgi formu, sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı, çevrimiçi ortamın değerlendirilmesine yönelik uzman görüş formu, öğrencilerin ortam hakkındaki görüşlerine yönelik açık uçlu anket formu ve öğrencilerin eğitim hakkındaki görüşlerine yönelik açık uçlu anket formu kullanılmıştır.

Kişisel bilgi formu. Araştırmanın pilot ve asıl uygulama süreçleri için araştırmacı tarafından geliştirilen kişisel bilgi formlarında; kişinin daha önce bilgi güvenliği hakkında bir eğitim alıp almadığı, interneti kullanım amaçları gibi sorular yer almaktadır (EK-A, EK-B). Kişisel bilgi formları çevrimiçi ortamda gönüllülük esasına uygun olarak uygulanmış olup, yine öğrenci velilerinden gerekli izinler alınmıştır.

Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı. Ortaokul öğrencilerine yönelik sanal ortamlarda bilgi güvenliği düzeylerini ölçmek amacıyla alanyazın taraması gerçekleştirilmiş, kapsama dahil edilmesi gereken temalar belirlenmiştir. Bu temalar doğrultusunda 16 açık uçlu sorudan oluşan bir ölçme aracı geliştirilmiştir. Soruların anlaşılabilirliği ve öğrenci seviyesine uygunluğunu belirlemek amacıyla dokuz altıncı sınıf öğrencisinin soruları değerlendirmesi istenmiştir. Öğrencilerden gelen geribildirimler doğrultusunda

öğrencilerin seviyesine uygun olmadığı düşünülen iki soru ölçme aracından çıkartılmıştır. 14 soruluk ölçme aracında (EK-C) yer alan sorular ve dereceli puanlama anahtarına yönelik bir değerlendirme yapılması için ise 10 alan uzmanına (Bilişim teknolojileri öğretmenlerine) başvurulmuştur. Uzmanlardan gelen geribildirimler doğrultusunda; benzer kazanımları ölçtüğü düşünülen ve kapsam geçerlik oranının düşük olduğu belirlenen üç soru ölçme aracından çıkartılmış, bazı sorularda ise çeşitli düzenlemeler gerçekleştirilmiştir. 11 soruya indirgenen ölçme aracında (EK-Ç) yer alması planlanan her soru için kapsam geçerlik oranı hesaplanmıştır. Nihai ölçme aracı maddeleri ve kapsam geçerlik oranları Tablo 40'ta verilmiştir.

Tablo 40

Ölçme Aracı Maddelerinin Kapsam Geçerliği Oranları

Sıra No	Hedeflenen Kazanım	KGO
1	Kişisel verinin ne anlama geldiğini bilir. Kişisel veri kapsamına giren bilgileri örneklendirebilir.	0.8
2	İnternette doğru bilgiye ulaşma yollarını bilir.	0.6
3	Sosyal ağlarda paylaşılmaması gereken bilgilerin farkına varır.	0.8
4	Siber zorbalık kavramı hakkında bilgi edinir. Hangi eylemlerin siber zorbalık kapsamına girdiğini bilir.	0.8
5	İnternette etkili arama yöntemlerini bilir.	0.6
6	Güçlü şifre oluşturma yöntemlerini bilir.	1
7	Web sayfalarındaki güvenli iletişim yolu kullanımını anlayabilir.	1
8	Siber zorbalığa maruz kaldığında ne yapacağın bilir.	0.6
9	Sosyal ağlarda alınabilecek güvenlik önemlerini bilir.	0.8
10	İnternet bilgi ağlarında yer alan bilgilerin doğrulunu sorgular.	0.8
11	İnternette paylaşılmaması gereken bilgilerin farkına varır.	0.8

Başarı testlerinde kapsam geçerlik oranının (KGO) tespitinden sonra, kapsam geçerlik indeksi (KGİ) testin tamamı için hesaplanır. Bu araştırma kapsamında geliştirilen çevrimiçi güvenlik ve risk düzeyi belirleme aracında yer almasına karar verilen maddelerin KGO değerlerinin ortalaması hesaplanarak KGİ değeri elde edilmiştir (KGİ=0,94). Başvurulan uzman sayısı 10 olduğu için, kapsam geçerlik ölçütü 0,62 olarak kabul edilmiştir. KGİ > KGÖ olduğundan, testin kapsam geçerliğinin istatistiksel olarak anlamlı olduğuna karar verilmiştir.

Başarı testinin dil bilgisi açısından değerlendirilmesi için ise iki dil bilgisi uzmanının (Türkçe ve Edebiyat öğretmeni olmak üzere iki uzman) görüşlerine başvurulmuştur. Uzmanlardan gelen geribildirimler doğrultusunda gerekli düzenlemeler yapılmıştır. Ölçme aracının son halinde yer alan soruların

değerlendirme ölçütlerine yönelik ise bir uzman görüş formu hazırlanmış, bu form yine 10 alan uzmanınca (Bilişim teknolojileri öğretmenleri) değerlendirilmiştir (EK-D).

Çevrimiçi ortamın değerlendirilmesine yönelik uzman görüş formu. Ortamın değerlendirilmesinde dikkate alınacak içeriğe yönelik ölçütlerin yer aldığı bir uzman görüş formu uzman görüşleri doğrultusunda (Bilgisayar ve öğretim teknolojileri anabilim dalında doktorasını tamamlamış ve bilgi güvenliğine yönelik çalışmaları olan iki akademisyen) araştırmacı tarafından hazırlanmıştır (EK-E). Ortam tasarımına yönelik ölçütler listesi için ise; Eren ve Erdem'in (2020); çocukları çevrimiçi güvenlik ve önlemler konusunda bilinçlendirmeye yönelik oluşturulan çevrimiçi çoklu ortamların nasıl olması gerektiği ve var olan sitelerin bu özellikler kapsamındaki durumunu ortaya koymak amacıyla gerçekleştirdiği ölçütler listesinin kullanılmasına karar verilmiş; bu amaçla gerekli izinler alınmıştır.

Öğrencilerin ortam hakkındaki görüşlerine yönelik açık uçlu anket formu. Araştırma kapsamında kullanılan çevrimiçi öğrenme ortamının katılımcılar tarafından nasıl kullanıldığının ve etkililiğin belirlenebilmesi amacıyla uzman görüşleri (Bilgisayar ve öğretim teknolojileri anabilim dalında doktorasını tamamlamış iki akademisyen) de dikkate alınarak araştırmacı tarafından açık uçlu anket formu geliştirilmiştir (EK-F). Pilot uygulama sürecinin sonunda öğrencilerin ortam hakkındaki görüşlerine yönelik olarak geliştirilen açık uçlu anket formu öğrencilere uygulanmıştır. Bu formda yer alan sorulardan bir kısmı aşağıdaki şekilde örneklendirilebilir:

1. Sitenin ismi uygun mudur?

2. Sitede bulunan içerikler güncel midir?

3. Video ve anlatıların süresi ne kadar olmalıdır (daha uzun-kısa)?

Öğrencilerin eğitim hakkındaki görüşlerine yönelik açık uçlu anket formları. Geliştirilen ortamda yürütülen eğitimler sonrasında öğrencilerin almış oldukları eğitim hakkındaki görüşlerini belirleyebilmek amacıyla uzman görüşleri (Bilgisayar ve öğretim teknolojileri anabilim dalında doktorasını tamamlamış iki akademisyen) dikkate alınarak araştırmacı tarafından Deney Grubu I ve Deney Grubu II için ayrı olmak üzere açık uçlu anket formları geliştirilmiştir. Araştırmanın deneysel uygulama sürecinin sonunda öğrencilerin eğitim hakkındaki görüşlerine

yönelik geliştirilen açık uçlu anket formları (EK-G ve EK-Ğ) uygulanmıştır. Bu formlarda yer alan sorulardan bir kısmı aşağıdaki şekilde örneklendirilebilir:

1.Çevrimiçi öğrenme ortamının size bilgi güvenliği ile ilgili ne gibi katkılar sağladığını düşünüyorsunuz? Eğer katkı sağlamadığını düşünüyorsanız bu durumu nasıl açıklarsınız?

2.Çevrimiçi öğrenme ortamını kullandığınız süreçte içeriği kullanmak ve yorumlamakla ilgili ne gibi zorluklarla karşılaştınız?

3.Kullandığınız ortamın içeriğine yönelik önerileriniz nelerdir?

Deney Grubu II öğrencilerine uygulanan açık uçlu anket formunda, Deney Grubu I öğrencilerine uygulanan formdaki sorulara ek olarak aşağıdaki soru yer almaktadır:

“Video konferans aracını kullanarak katıldığınız eş zamanlı dersler size ne gibi katkılar sağladı?”

Verilerin Analiz Yöntemi

Araştırmanın ana hatları kapsamında alt problemler, yöntem bölümünde veri kaynakları, verilerin toplanması, verilerin analizine ilişkin bilgiler sunulmuştur (Bkz. Tablo 35).

Kullanılacak olan istatistik yöntemleri belirlenirken, öncelikle çalışma gruplarının normal dağılım gösterip göstermedikleri test edilmiştir. Bu kapsamda örneklem büyüklüğünün 50'den az olması sebebiyle Shapiro-Wilks testiyle normalik varsayımı sınanmıştır.

Çalışma kapsamında kullanılan açık uçlu anket formu verilerinin analizi için içerik analizi yöntemine başvurulmuştur. Açık uçlu anket formları çevrimiçi ortamda uygulanmıştır. Elde edilen metinlerden temalar oluşturulmuştur. Verilerin analizi için sırasıyla betimsel analiz ve içerik analizi yöntemlerine başvurulmuştur. Betimsel analizde, önceden belirlenen temalara göre veriler özetlenmekte ve yorumlanmaktadır. Açık uçlu anket formuna dayanarak gerçekleştirilmiş betimsel analizin aşamaları (Yıldırım & Şimşek, 2011) Tablo 41'de sunulmaktadır.

Tablo 41

Betimsel Analiz Sürecinin Aşamaları ve Yürütülen İşlemler

Aşamalar	Yürütülecek İşlemler
Betimsel analiz için çerçeve oluşturulması	Araştırma soruları doğrultusunda bir çerçevenin oluşturulması
Tematik çerçeveye göre verilerin işlenmesi	Yarı yapılandırılmış görüşme ve yansıma raporlarından elde edilen verilerin işlenmesi
Bulguların tanımlanması	Verilerin düzenlenmesi,
Bulguların yorumlanması	Bulgulara ilişkin açıklamaların yapılması, ilişkilere ve karşılaştırmalara yer verilmesi

Araştırmanın nitel verilerinin analizi sürecinde betimsel analize ek olarak içerik analizi kullanılmıştır. İçerik analiz sürecinde betimsel analiz ile edinilen verileri derinlemesine açıklayabilecek kavramlara ve ilişkilere ulaşılması hedeflenmektedir. Katılımcılarla yapılan açık uçlu anket formundan elde edilen temalar; iki ayrı kodlayıcı tarafından raporlanmış olup, yapılan karşılaştırmadan sonra ortak temalar derlenmiştir.

Bölüm 4.
Bulgular

Bu bölümde, araştırmanın asıl uygulama sürecinde elde edilen bulgular sunulmuştur. Araştırmanın asıl uygulama süreci Ankara ilinde merkezi bir ortaokulda öğrenim görmekte olan altıncı sınıf öğrencileriyle çevrimiçi ortamda yürütülmüştür. Uygulama sürecinde veri toplama aracı olarak; kişisel bilgi formu, ön-test, son-test ve kalıcılık testi (Sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracı) ile açık uçlu anket formlarına başvurulmuştur. Veri toplama araçlarından elde edilen bulgular alt başlıklar halinde sunulmuştur.

Çalışma gruplarının ön-test sonuçları incelendiğinde; öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin bilgi düzeylerinin ölçme aracına göre ortalamanın üzerinde olduğu, ancak öğrencilerin bilgi güvenliği ile ilgili daha kapsamlı bir eğitime katılmalarının daha fazla katkı sağlayacağı düşünülmüştür. Nitekim öğrenciler beşinci sınıf düzeyinde, "Bilişim Teknolojileri ve Yazılım" dersi kapsamında bilgi güvenliği ile ilgili olarak birtakım kazanımlara (Bkz. Tablo 37) yönelik eğitimler almaktadırlar (MEB Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı, 2018). Araştırma kapsamında geliştirilen çevrimiçi ortamda ise; kişisel verilerin korunması, sosyal ağların kullanımı, internet okuryazarlığı, siber zorbalık, çevrimiçi riskler, şifre güvenliği, zararlı yazılımlar, web güvenlik önlemleri ve güvenli olmayan iletişim yolları konularına yönelik kapsamlı bilgiler sunulmuş olup, "etkinlikler", "kendimizi sınayalım" ve "oyunlar" bölümleriyle konuların pekiştirilmesi amaçlanmıştır.

Katılımcıların Sanal Ortamlarda Bilgi Güvenliğine İlişkin Bilgi Düzeyleri

Araştırmanın ilk sorusu "*Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri nedir?*" şeklindedir. Bu soruya yanıt alabilmek amacıyla ön-test, son-test ve kalıcılık testine başvurulmuştur. Araştırmaya katılan öğrencilerin ön-testten aldıkları puanlar EK-J ve EK-K'de; son-testten aldıkları puanlar EK-L ve EK-M'de; kalıcılık testinden aldıkları puanlar EK-N ve EK-O'da sunulmuştur. Araştırmanın çalışma gurubunu oluşturan Deney Grubu I ve Deney Grubu II öğrencilerine ait ön-test; son-test ve kalıcılık testi puanları ortalamaları ise Tablo 42' de verilmiştir.

Tablo 42

Deney Grubu I ve Deney Grubu II Öğrencilerinin Ön-test; Son-Test ve Kalıcılık Testi Ortalamaları

Grup	Ön-Test Ortalaması	Son-Test Ortalaması	Kalıcılık Testi Ortalaması
Deney Grubu I	75.00	90.00	84.69
Deney Grubu II	72.54	89.53	90.65

Katılımcıların Bilgi Güvenliği Hakkında Daha Önce Yüz Yüze Ortamda Bir Eğitim Alma Durumunun Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeylerine Etkisi

Araştırmanın ikinci sorusu "*Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri, bilgi güvenliği hakkında daha önce yüz yüze ortamda bir eğitim alma durumuna göre nasıl değişmektedir?*" şeklindedir. Bu soruya yanıt alabilmek amacıyla kişisel bilgi formu ve sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracına başvurulmuştur.

Kişisel bilgi formu aracılığıyla; bilgi güvenliği hakkında daha önce bir eğitim alma durumlarına yönelik veriler toplanmıştır. Öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin ölçülmesi için ise araştırmacı tarafından geliştirilen sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracına başvurulmuştur.

Verilerin analizi sürecinde bilgisayar tabanlı bir istatistik programından faydalanılmıştır. Öğrencilerin kişisel bilgilerinin belirlenmesinde betimsel analizlerden faydalanılmıştır. Çalışma gruplarının ön-teste dayalı olarak çevrimiçi güvenlik ve risk ile ilgili bilgi düzeylerinin normal dağılım gösterip göstermediğini belirlemek amacıyla kullanılan Shapiro-Wilks testi sonuçları Tablo 43'de verilmiştir.

Tablo 43

Ön-Test Sonuçlarına İlişkin Shapiro-Wilks Normallik Testi Sonuçlarının Dağılımı

Grup	Df	p
Deney Grubu I	26	0.10
Deney Grubu II	26	0.02

Tablo 43'de görüldüğü üzere; Deney Grubu I öğrencilerine ilişkin ön-test puanlarının normal dağılım gösterdiği ($p>.05$), ancak Deney Grubu II öğrencilerine ilişkin ön-test puanlarının normal dağılım göstermediği ($p<.05$) belirlenmiştir. Bu

doğrultuda grupların ön-test puanları bağlamında denk olup olmadığının belirlenebilmesi amacıyla parametrik olmayan istatistiksel yöntemlerden ilişkisiz ölçümler için Mann-Whitney U-Testinin kullanımının uygun olduğuna karar verilmiştir. Uygulanan Mann-Whitney U-Testinin sonuçları Tablo 44'te verilmiştir.

Tablo 44

Deney Grubu I ve Deney Grubu II Öğrencilerinin Ön-Test Sonuçlarının Karşılaştırılmasına İlişkin Mann-Whitney U-Testi Sonuçlarının Dağılımı

Grup	N	Sıra Ortalaması	Sıra Toplamı	u	p
Deney Grubu I	26	26.65	693.00	334	.94
Deney Grubu II	26	26.35	685.00		

Tablo 44'teki veriler doğrultusunda, araştırmanın çalışma grubunu oluşturan gruplar arasında ön-test puanları açısından anlamlı bir fark olmadığı belirlenmiştir (p>.05). Bu bulgu, grupların sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri açısından denk oldukları şeklinde yorumlanmıştır.

Öğrencilerin bilgi güvenliği hakkında daha önce yüz yüze ortamda eğitim alma durumunun sanal ortamlarda bilgi güvenliğine ilişkin düzeylerine etkisinin belirlenmesi amacıyla kişisel bilgi formu ve sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracına başvurulmuştur. Bu amaç doğrultusunda Deney Grubu I öğrencilerinin ön -test puanlarının normal dağılım göstermesi (p>05) sebebiyle bağımsız gruplar t-testinin kullanılmasının uygun olduğuna karar verilmiştir. Deney Grubu I öğrencilerinin bilgi güvenliği hakkında yüz yüze ortamda eğitim alma durumunun sanal ortamlarda bilgi güvenliğine ilişkin bilgi düzeylerine etkisinin belirlenmesi amacıyla gerçekleştirilen bağımsız gruplar t-testi sonuçları Tablo 45'te verilmiştir:

Tablo 45

Deney Grubu I Öğrencilerinin Bilgi Güvenliği Hakkında Daha Önce Yüz Yüze Ortamda Eğitim Alma Durumu ve Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeylerine Göre Bağımsız Gruplar t-testi Sonuçlarının Dağılımı

Yüz Yüze Eğitim Alma Durumu	N	X	S	sd	t	p
Yüz yüze bir eğitime katıldım.	20	73.10	16.02	24	1.09	.28
Yüz yüze birkaç eğitime katıldım.	6	81.33	16.90			

Tablo 45'te görüldüğü üzere ön-test verileri doğrultusunda Deney Grubu I için analiz sonuçları, öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin; bilgi güvenliği hakkında daha önce yüz yüze ortamda bir eğitim alma durumuna bağlı olarak değişmediğini göstermektedir, $t(24)= 1.09$, $p>.05$.

Deney Grubu II öğrencilerinin ön-test sonuçlarının normal dağılım göstermemesi ($p<.05$) sebebiyle, öğrencilerin bilgi güvenliği hakkında yüz yüze ortamda eğitim alma durumu ile sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri arasındaki ilişkinin belirlenmesi amacıyla Mann-Whitney U Testinin kullanılmasının uygun olduğuna karar verilmiştir. Deney Grubu II için uygulanan Mann-Whitney U Testi sonuçları Tablo 46'da verilmiştir:

Tablo 46

Deney Grubu II Öğrencilerinin Bilgi Güvenliği Hakkında Yüz Yüze Ortamda Eğitim Alma Durumu ve Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeylerinin Göre Mann-Whitney U Testi Sonuçlarının Dağılımı

Yüz Yüze Eğitim Alma Durumu	N	Sıra Ortalaması	Sıra Toplamı	U	P
Yüz yüze bir eğitime katıldım.	17	12.94	220.00	67.00	.60
Yüz yüze birkaç eğitime katıldım.	9	14.56	131.00		

Tablo 46'da görüldüğü üzere ön-test verileri doğrultusunda Deney Grubu II için analiz sonuçları, öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin; bilgi güvenliği hakkında daha önce yüz yüze ortamda bir eğitim alma durumuna göre değişmediğini göstermektedir ($p>.05$).

Katılımcıların Bilgi Güvenliği Hakkında Daha Önce Çevrimiçi Ortamda Eğitim Alma Durumunun Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeylerine Etkisi

Araştırmanın üçüncü sorusu "*Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri, bilgi güvenliği hakkında daha önce çevrimiçi ortamda bir eğitim alma durumuna göre nasıl değişmektedir?*" şeklindedir. Öğrencilerin bilgi güvenliği hakkında daha önce çevrimiçi ortamda eğitim alma durumunun sanal ortamlarda bilgi güvenliğine ilişkin düzeylerine etkisinin belirlenmesi amacıyla kişisel bilgi formu ve sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracına başvurulmuştur. Bu amaç doğrultusunda Deney Grubu I öğrencilerinin ön-test puanlarının normal dağılım göstermesi (p>.05) sebebiyle tek yönlü ANOVA testinin kullanılmasının uygun olduğuna karar verilmiştir. Deney Grubu I için uygulanan tek yönlü ANOVA testinin sonuçları Tablo 47'de verilmiştir.

Tablo 47

Deney Grubu I Öğrencilerinin Bilgi Güvenliği Hakkında Daha Önce Çevrimiçi Ortamda Eğitim Alma Durumu ve Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeylerine Göre Tek Yönlü ANOVA Testi Sonuçlarının Dağılımı

Varyansın Kaynağı	Kareler Toplamı	sd	Kareler Ortalaması	F	p
Gruplararası	426.75	2	213.37	0.79	.46
Gruplariçi	6191.25	3	269.18		
Toplam	6618.00	25			

Tablo 47'de görüldüğü üzere; öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri arasında bilgi güvenliği hakkında daha önce çevrimiçi ortamda eğitim alma durumuna (Hiç eğitim almadım, Bir kez eğitim aldım, Birkaç kez eğitim aldım) bağlı olarak anlamlı bir fark olmadığı belirlenmiştir (p>.01).

Deney Grubu II öğrencilerinin ön-test sonuçlarının normal dağılım göstermemesi (p<.05) sebebiyle, bilgi güvenliği hakkında daha önce çevrimiçi ortamda eğitim alma durumu ile sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri arasındaki ilişkinin belirlenmesi amacıyla Kruskal Wallis H-Testi analizine başvurulmuştur. Deney grubu II için uygulanan Kruskal Wallis H-Testi analizi sonuçları Tablo 48'de verilmiştir:

Tablo 48

Deney Grubu II Öğrencilerinin Bilgi Güvenliği Hakkında Daha Önce Çevrimiçi Ortamda Eğitim Alma Durumu ve Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeylerine Göre Kruskal Wallis H-Testi Analizi Sonuçlarının Dağılımı

Çevrimiçi Eğitim Alma Durumu	n	Sıra Ortalaması	sd	X^2	p	Anlamlı Fark
Hiç eğitim almadım.	16	13.94	2	1.17	.91	-
Çevrimiçi bir eğitime katıldım.	6	13.17				
Çevrimiçi birkaç eğitime katıldım.	4	12.25				

Tablo 48'de görüldüğü üzere ön-test verileri doğrultusunda Deney Grubu II için analiz sonuçları, öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin; bilgi güvenliği hakkında daha önce çevrimiçi ortamda bir eğitim alma durumuna göre değişmediğini göstermektedir, x^2 (sd=2, n=26) = 1.17, p>.05.

Sanal Ortamlarda Bilgi Güvenliği ile İlgili Eğitime Yönelik Tasarlanan Ortamda Yürütülen Eğitimlerin Ortaokul Öğrencilerinin Sanal Ortamlarda Bilgi Güvenliği ile İlgili Bilgi Durumlarındaki Değişimine Etkisi

Araştırmanın dördüncü araştırma sorusu "*Sanal ortamlarda bilgi güvenliği ile ilgili eğitime yönelik tasarlanan ortamda yürütülen eğitimlerin ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliği ile ilgili bilgi durumlarındaki değişimine etkisi nedir?*" şeklindedir. Bu soruya yanıt alabilmek amacıyla sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracına başvurulmuştur. Çalışma gruplarının sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin normal dağılım gösterip göstermediğini belirlemek amacıyla son-test verilerine yönelik uygulanan Shapiro-Wilks testi sonuçları ise Tablo 49'da verilmiştir:

Tablo 49

Son-Test Sonuçlarına İlişkin Shapiro-Wilks Normallik Testi Sonuçlarının Dağılımı

Uygulanan Test	Df	p
Deney Grubu I	26	0.27
Deney Grubu II	26	0.11

Tablo 49'da görüldüğü üzere; son-teste yönelik olarak Deney grubu I ve Deney Grubu II için verilerin normal dağılım gösterdiği belirlenmiştir (*p*>.05). Araştırma kapsamında yürütülen deneysel uygulamanın katılımcıların sanal

ortamlarda bilgi güvenliğine ilişkin düzeyleri üzerindeki etkililiğinin test edilmesi için öğrencilere ait ön-test ve son-test puanları karşılaştırılmıştır. Deney grubu I öğrencilerinin ön-test ve son-test puanları normal dağılım gösterdiğinden (*p*>05); ön-test ve son test puanlarının karşılaştırılması amacıyla parametrik istatistik yöntemlerinin kullanılmasına karar verilmiştir. Deney grubu II öğrencilerinin ön-test puanlarının normal dağılım göstermemesi ve son-test puanlarının normal dağılım göstermesi sebebiyle; ön-test ve son-test puanlarının karşılaştırılması amacıyla parametrik olmayan istatistik yöntemlerinden Wilcoxon İşaretli Sıralar Testi'nin kullanımının uygun olduğuna karar verilmiştir.

Deney Grubu I öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin eğitim öncesinde ve sonrasında anlamlı bir farklılık gösterip göstermediğine ilişkin bağımlı gruplar t-testi sonuçları Tablo 50'de verilmiştir.

Tablo 50

Deney Grubu I Öğrencilerinin Ön-test ve Son-test Sonuçlarının Karşılaştırılmasına İlişkin Bağımlı Gruplar t-testi Sonuçlarının Dağılımı

Test	N	X	S	sd	t	P
Ön-Test	26	75.00	16.27	25	4.88	.00
Son-Test	26	90.00	14.08			

Tablo 50'de görüldüğü üzere; öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin eğitim sonrasında anlamlı bir artış gösterdiği belirlenmiştir, $t(25) = 4.88$, $p < .05$. Bu sonuçlar doğrultusunda, bilgi güvenliği ilgili olarak çevrimiçi ortamda alınan kapsamlı bir eğitimin öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerini geliştirmede anlamlı bir etkisinin olduğu söylenebilir.

Deney Grubu II öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin eğitim öncesinde ve sonrasında anlamlı bir farklılık gösterip göstermediğine ilişkin uygulanan Wilcoxon işaretli sıralar testi sonuçları Tablo 51'de verilmiştir.

Tablo 51

Deney Grubu II Öğrencilerinin Ön-test ve Son-test Sonuçlarının Karşılaştırılmasına İlişkin Wilcoxon İşaretli Sıralar Testi Sonuçlarının Dağılımı

Son-Test - Ön-Test	n	Sıra Ortalaması	Sıra Toplamı	z	p
Negatif Sıra	5	6.10	30.50	3.68*	.00
Pozitif Sıra	21	15.26	320.50		

*Negatif sıralar temeline dayalı

Tablo 51'e göre, analiz sonuçları, Deney Grubu II öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri açısından eğitim öncesi ve sonrası puanları arasında anlamlı bir fark olduğunu göstermektedir (z= 3.68, p<.05). Fark puanlarının sıra ortalaması ve toplamları dikkate alındığında, gözlemlenen bu farkın son-test puanı lehine olduğu görülmektedir. Bu sonuçlar doğrultusunda, bilgi güvenliği ile ilgili olarak çevrimiçi ortamda alınan kapsamlı bir eğitimin öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerini geliştirmede anlamlı bir etkisinin olduğu söylenebilir.

Çevrimiçi Ortamda Yürütülen Bilgi Güvenliği ile İlgili Eğitimlerin Öğrenilenlerin Kalıcılığına Etkisi

Araştırmanın beşinci araştırma sorusu "*Çevrimiçi ortamda yürütülen bilgi güvenliği ile ilgili eğitimlerin öğrenilenlerin kalıcılığına etkisi nedir?*" şeklindedir. Bu soruya yanıt alabilmek amacıyla kalıcılık testinden faydalanılmıştır. Araştırmanın asıl uygulama sürecinde kalıcılık testinden alınan puanlar Ek 15 ve Ek 16'da verilmiştir. Çalışma gruplarının sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin normal dağılım gösterip göstermediğini belirlemek amacıyla kalıcılık testi verilerine yönelik uygulanan Shapiro-Wilks testinin sonuçları Tablo 52'de verilmiştir.

Tablo 52

Kalıcılık Testi Sonuçlarına İlişkin Shapiro-Wilks Normallik Testi Sonuçları

Grup	Df	p
Deney Grubu I	26	.11
Deney Grubu II	26	.01

Tablo 52'de görüldüğü üzere; son-teste yönelik olarak, Deney Grubu I öğrencileri için p>.05 ve Deney Grubu II öğrencileri için p<.05 olarak belirlenmiş, bu

anlamda Deney Grubu I için parametrik; Deney Grubu II için parametrik olmayan istatistiksel yöntemlerin kullanımının uygun olduğuna karar verilmiştir.

Araştırma kapsamında yürütülen deneysel uygulamanın katılımcıların sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerinin kalıcılığı üzerindeki etkililiğinin test edilmesi için Deney Grubu I ve Deney Grubu II öğrencilerine ait son-test ve kalıcılık testi puanları karşılaştırılmıştır. Deney Grubu I öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin son-test ve kalıcılık testi puanları açısından anlamlı bir farklılık gösterip göstermediğine ilişkin bağımlı gruplar t-testi sonuçları Tablo 53'te verilmiştir.

Tablo 53

Deney Grubu I Öğrencilerinin Son-test ve Kalıcılık Testi Sonuçlarının Karşılaştırılmasına İlişkin Bağımlı Gruplar t-testi Sonuçlarının Dağılımı

Test	n	X	S	sd	t	p
Son-Test	30	90.00	14.08	25	1.92	.06
Kalıcılık Testi	30	84.69	14.27			

Tablo 54'e göre analiz sonuçları; Deney Grubu I öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin son-test ve kalıcılık testi puanları açısından anlamlı bir fark olmadığını göstermektedir, $t(25)=1.92$, $p>.01$. Bu durum; araştırma kapsamında yürütülen eğitimin, katılımcıların sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerinin kalıcılığını sağladığı şeklinde yorumlanabilir.

Deney Grubu II öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri son-test ve kalıcılık testi puanları açısından anlamlı bir farklılık gösterip göstermediğine ilişkin Wilcoxon işaretli sıralar testi sonuçları ise Tablo 54'te verilmiştir.

Tablo 54

Deney Grubu II Öğrencilerinin Son-Test ve KalıcılıkTesti Sonuçlarının Karşılaştırılmasına İlişkin Wilcoxon İşaretli Sıralar Testi Sonuçları

Son-Test – Kalıcılık Testi	n	Sıra Ortalaması	Sıra Toplamı	z	p
Negatif Sıra	10	12.65	126.50	.00	1.00
Pozitif Sıra	12	10.54	126.50		
Bağlantı	4				

*Negatif sıralar temeline dayalı

Tablo 54'e göre analiz sonuçları, Deney Grubu II öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri açısından son-test ve kalıcılık testi puanları arasında anlamlı bir fark olmadığını göstermektedir (z=.00, p>.05). Bu durum, araştırma kapsamında yürütülen eğitimin katılımcıların sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerinin kalıcılığını sağladığı şeklinde yorumlanabilir.

Çevrimiçi Ortamda Eş Zamansız Eğitimlere Katılan Ortaokul ile Eş Zamansız Eğitimlere Ek Olarak Eş Zamanlı Eğitimlere Katılan Öğrencilerin Sanal Ortamlarda Bilgi Güvenliğine Yönelik Öğrenmeleri

Araştırmanın altıncı araştırma sorusu "*Çevrimiçi ortamda eş zamansız eğitimlere katılan ortaokul öğrencileri ile eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliğine yönelik öğrenmeleri açısından istatistiksel olarak anlamlı bir fark var mıdır?*" şeklindedir. Bu soruya yanıt alabilmek amacıyla Deney Grubu I ve Deney Grubu II öğrencilerine yönelik uygulanan son-test puanlarının normal dağılım gösterdiği belirlenmiştir (p>.05). Bu doğrultuda Deney Grubu I ve Deney Gurubu II öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri arasındaki ilişkinin belirlenebilmesi amacıyla başvurulan bağımsız gruplar t-testi sonuçları Tablo 55'te verilmiştir.

Tablo 55

Deney Grubu I ve II Öğrencilerinin Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeylerine Göre Bağımsız Gruplar t-testi Sonuçları

Çalışma Grubu	n	X	ss	df	t	p
Deney Grubu I	26	90.00	14.08	50	.10	.92
Deney Grubu II	26	89.53	18.61			

Tablo 55'teki veriler doğrultusunda Deney Grubu I ve II öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin; geliştirilen çevrimiçi ortamdaki eğitimlere ek olarak video konferans aracı ile eş zamanlı eğitim alınıp alınmama durumuna bağlı olarak değişmediği görülmektedir, t(50)=.10, p>.01. Bu durum; tasarlanan ortamda verilen eğitimlerin herhangi bir eş zamanlı ortama ihtiyaç duyulmaksızın öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerine katkı sağladığı şeklinde de yorumlanabilir. Yine; Deney Grubu I ve II öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri açısından herhangi bir farkın bulunamaması; öğrencilerin eş zamanlı derslere katılım düzeylerinden kaynaklandığı düşünülebilir (Bkz. Tablo 33).

Çevrimiçi Ortamda Eş Zamansız Eğitimlere Katılan Öğrenciler ile Eş Zamansız Eğitimlere Ek Olarak Eş Zamanlı Eğitimlere Katılan Öğrencilerin Sanal Ortamlarda Bilgi Güvenliğine Yönelik Öğrendiklerinin Kalıcılığı

Araştırmanın yedinci araştırma sorusu "*Çevrimiçi ortamda eş zamansız eğitimlere katılan öğrenciler ile eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliğine yönelik öğrenilenlerin kalıcılığı açısından istatistiksel olarak anlamlı bir fark var mıdır?*" şeklindedir. Bu amaçla uygulanan Shapiro-Wilks testi sonuçları doğrultusunda, Deney Grubu I öğrencilerinin kalıcılık testi puanlarının normal dağılım gösterdiği, ancak Deney Grubu II öğrencilerinin kalıcılık testi puanlarının normal dağılım göstermediği belirlenmiştir (Bkz. Tablo 52). Bu sonuçlar doğrultusunda grupların kalıcılık testi puanlarının karşılaştırılmasına ilişkin parametrik olmayan istatistiksel yöntemlerden Mann-Whitney U testi kullanımına karar verilmiştir.

Deney Grubu I ve Deney Gurubu II öğrencilerinin eğitim sonrasında sanal ortamlarda bilgi güvenliğine ilişkin bilgilerinin kalıcılığı arasındaki ilişkiye yönelik Mann-Whitney U testi sonuçları Tablo 56'da verilmiştir.

Tablo 56

Deney Grubu I ve Deney Gurubu II Öğrencilerinin Eğitim Sonrasında Sanal Ortamlarda Bilgi Güvenliğine İlişkin Bilgilerinin Kalıcılığı Arasındaki İlişkiye Göre Mann-Whitney U Testi Sonuçlarının Dağılımı

Grup	n	Sıra Ortalaması	Sıra Toplamı	u	p
Deney Grubu I	26	22.98	597.50	246.50	.09
Deney Grubu II	26	30.02	780.50		

Tablo 56'daki veriler doğrultusunda, araştırmanın çalışma grubunu oluşturan deney gruplarının kalıcılık testinden elde etmiş oldukları puanlar açısından anlamlı bir fark olmadığı belirlenmiştir (p>.05). Bu bulgu, grupların sanal ortamlarda bilgi güvenliği ile ilgili bilgilerinin kalıcılığı açısından denk oldukları şeklide yorumlanabilir.

Sanal Ortamlarda Bilgi Güvenliği ile İlgili Olarak Çevrimiçi Ortamda Yürütülen Eğitimlere Katılan Öğrencilerin Aldıkları Eğitime Yönelik Görüşleri

Araştırmanın sekizinci ve son araştırma sorusu "*Sanal ortamlarda bilgi güvenliği ile ilgili olarak çevrimiçi ortamda yürütülen eğitimlere katılan öğrencilerin aldıkları eğitime yönelik görüşleri nelerdir?*" şeklindedir. Bu amaç doğrultusunda çevrimiçi

ortamdaki eğitimlerin ve son testin uygulanmasından sonra; öğrencilerin eğitime ve tasarlanan ortama yönelik görüşlerini belirleyebilmek amacıyla Deney Grubu I ve Deney Grubu II için ayrı ayrı olmak üzere açık uçlu anket formları uygulanmıştır. Deney Grubu I ve Deney Grubu II için uygulanan formlarda ortak sorular yer alması sebebiyle, sonuçlar tek tabloda derlenmiştir. Açık uçlu anket formu aracılığıyla elde edilen veriler alt başlıklar halinde sunulmuştur:

Açık uçlu anket formu bulguları. Deney Grubu I'de 26 öğrenci ve Deney Grubu II'de 26 olmak üzere toplam 52 öğrenci açık uçlu anket formunu yanıtlamıştır. Açık uçlu anket formu aracılığıyla elde edilen veriler alt başlıklar halinde sunulmuştur:

Ortamın sanal ortamlarda bilgi güvenliğine ilişkin sağladığı katkılara yönelik yorumlar. Çevrimiçi öğrenme ortamının sanal ortamlarda bilgi güvenliğine ilişkin sağladığı katkılara yönelik belirlenen temalar ve frekansları Tablo 57'de verilmiştir.

Tablo 57

Ortamın Sanal Ortamlarda Bilgi Güvenliğine İlişkin Sağladığı Katkılara Yönelik Yanıtların Dağılımı

Tema	%	f
Yeni bilgilerin öğrenilmesi	44,23	23
İnternetin bilinçli ve güvenli kullanımı	28,85	15
Bilgiye kolay erişim	7,69	4
Bilgisayarların bilinçli ve güvenli kullanımı	3,85	2
Siber zorbalık farkındalığı kazandırılması	3,85	2
Kişisel bilgilerin korunması	1,92	1
Hesap güvenliği	1,92	1
Katkı sağlamadı.	1,92	1
Bilmiyorum.	5,77	3
Toplam Temaların Sayısı	100,00	52

Tablo 57 incelendiğinde, öğrencilerin büyük çoğunluğunun (48) çevrimiçi öğrenme ortamının sanal ortamlarda bilgi güvenliğine ilişkin katkı sağladığını belirttiği görülmektedir. Ortamın sanal ortamlarda bilgi güvenliğine ilişkin ne gibi katkılar sağladığına yönelik ise, "İnternetin bilinçli ve güvenli kullanımı, bilgiye kolay erişim, bilgisayarların bilinçli ve güvenli kullanımı, siber zorbalık farkındalığı kazandırılması, kişisel bilgilerin korunması, hesap güvenliği" temaları dikkat çekmektedir.

Ortamda sunulan içeriğin kullanımı ile ilgili karşılaşılan zorluklara yönelik yorumlar. Ortamda sunulan **i**çeriği kullanmak ile ilgili karşılaşılan zorluklarla yönelik olarak belirlenen temalar ve frekansları Tablo 58'de verilmiştir.

Tablo 58

Ortamda Sunulan İçeriğin Kullanımı ile İlgili Karşılaşılan Zorluklara Yönelik Yanıtların Dağılımı

Tema	%	f
Herhangi bir zorlukla karşılamadım.	90,38	47
"Yorumlar" bölümüne yönelik sorunlar	3,85	2
Siteye giriş şifrelerinin uzun olması	1,92	1
İçeriği kullanmak ve yorumlamak konusunda zorlandım.	1,92	1
Tamamlanan bölümlerin bazen "tamamlanmadı" görünmesi	1,92	1
Toplam Temaların Sayısı	100,00	52

Tablo 58 incelendiğinde, öğrencilerin büyük çoğunluğunun (47) çevrimiçi öğrenme ortamında sunulan içeriğin kullanımı ile ilgili herhangi bir zorlukla karşılaşmadığı görülmektedir. İki öğrencinin "Yorumlar" bölümüne yönelik karşılaştıkları sorunlara yönelik ifadeleri şu şekildedir:

> *"Yaptığımız yorumlar yorumu yapan kişi tarafından silinebilir hale getirilebilir."* Deney Grubu II-Öğrenci 6

> *"Bazen konuşmalar çok lakayt olabiliyor insanlar birbirlerine saygı duymadan cevap verebiliyor"* Deney Grubu II-Öğrenci 22

İçeriğin kullanımı ile ilgili karşılaşılan zorluklara yönelik diğer temalar; "Siteye giriş şifrelerinin uzun olması, içeriği kullanmak ve yorumlamak konusunda zorlandım, tamamlanan bölümlerin bazen 'tamamlanmadı' görünmesi" şeklindedir.

Ortamın içeriğine yönelik öneriler. Kullanılan ortamın içeriğine yönelik olarak belirlenen temalar ve frekansları Tablo 59'da verilmiştir.

Tablo 59

Ortamın İçeriğine Yönelik Önerilerin Dağılımı

Tema	%	f
Herhangi bir önerim yok.	61,54	32
Video eklenmesi.	13,46	7
Yeni içerik eklenmesi	9,62	5
Kolay erişimin sağlanması	3,85	2
Soruların çoğaltılması.	1,92	1
Metin formatında içeriklerin yer alması.	1,92	1
İçeriklerin yaygınlaştırılması.	1,92	1
Oyun eklenmesi	1,92	1
Öğrencilerin yorumlarda daha özenli olması	1,92	1
Testlerdeki cevaplarda oluşan hataların giderilmesi	1,92	1
Toplam Temaların Sayısı	**100,00**	**52**

Tablo 59 incelendiğinde, öğrencilerin büyük çoğunluğunun (32) ortamın içeriğine yönelik herhangi bir önerisinin olmadığı görülmektedir. Ortamın içeriğine yönelik öneriler kapsamında elde edilen; "Videoların çoğaltılması (7) ve Yeni içerik eklenmesi (4) önerileri dikkat çekmektedir. Ortamın içeriğine yönelik diğer öneriler ise; "Kolay erişimin sağlanması, soruların çoğaltılması, metin formatında içeriklerin yer alması, içeriklerin yaygınlaştırılması, oyun eklenmesi, öğrencilerin yorumlarda daha özenli olması ve testlerdeki cevaplarda oluşan hataların giderilmesi" şeklindedir.

Ortamın tasarımına yönelik öneriler. Kullanılan ortamın tasarımına yönelik olarak belirlenen temalar ve frekansları Tablo 60'ta verilmiştir.

Tablo 60

Ortamın Tasarımına Yönelik Önerilerin Dağılımı

Tema	%	f
Herhangi bir önerim yok.	78,85	41
Ortam tasarımının daha renkli hale getirilmesi	7,69	4
Kullanılabilirliğin sağlanması	11,54	6
Görsel ve videoların çoğaltılması	1,92	1
Toplam Temaların Sayısı	**100,00**	**52**

Tablo 60 incelendiğinde, öğrencilerin büyük çoğunluğunun (41) ortamın tasarımına yönelik olarak herhangi bir önerisinin olmadığı belirlenmiştir. Ortamın tasarımına yönelik öneriler kapsamında elde edilen temalar arasında; "Ortam tasarımının daha renkli hale getirilmesi (4) ve Kullanılabilirliğin sağlanması (6)" dikkat çekmektedir. Bir öğrenci ise "Görsel ve videoların çoğaltılması" yanıtını

vermiştir. “Ortam tasarımının daha renkli hale getirilmesi” temasına dahil edilen öğrenci görüşleri şu şekildedir:

> *“Yazılı anlatımlar yerine bence videolu anlatım yapılabilir ve arka plan daha canlı ve renkli yapılabilir.”* Deney Grubu I- Öğrenci 20
>
> *“Kullandığım ortamın tasarımına yönelik önerim sayfanın biraz daha renkli olması”* Deney Grubu II- Öğrenci 4
>
> *“Tasarımı sade ve güzel, ama biraz renk katılabilir.”* Deney Grubu I- Öğrenci 3
>
> *“Daha renkli daha şekilli olabilir.”* Deney Grubu II- Öğrenci 26

“Kullanılabilirliğin sağlanması” temasına dahil edilen öğrenci görüşleri şu şekildedir:

> *“Geçilen konular "geçildi" olarak işaretlenebilir. Bunların dışında çok iyi olmuş, elinize sağlık.”* Deney Grubu I- Öğrenci 26
>
> *“Oturumu kapat butonunun hesabım butonun yanına alınırsa daha güzel durabilir.”* Deney Grubu I- Öğrenci 14
>
> *“Kolay kullanılabilir olsun.”* Deney Grubu I- Öğrenci 17
>
> *“Daha anlaşılır olmalı.”* Deney Grubu I- Öğrenci 5
>
> *“Profil fotoğrafı ve hakkımızda bilgiler konulabilir ama bunlar çok gerekli şeyler değil.”* Deney Grubu II- Öğrenci 10
>
> *“Tasarım güzeldi renkleri benim ilgimi çekti belki puan kazanma eklenebilir.”* Deney Grubu II- Öğrenci 2

Video konferans aracı (zoom) kullanarak katılınan eş zamanlı derslerin sağladığı katkılara yönelik bulgular. Deney Grubu II öğrencileri, Deney Grubu I öğrencilerinden farklı olarak tasarlanan çevrimiçi ortamdaki dersleri takip etmenin yanısıra eş zamanlı derslere katılmışlardır. Bu doğrultuda, Deney Grubu I öğrencilerinden farklı olarak Deney Grubu II öğrencilerinin katıldığı eş zamanlı derslerin sağladığı katkılar araştırılmıştır. Video konferans aracı (zoom) kullanarak katılınan eş zamanlı derslerin katkılar sağladığı katkılara yönelik olarak belirlenen temalar ve frekansları Tablo 61’de verilmiştir.

Tablo 61

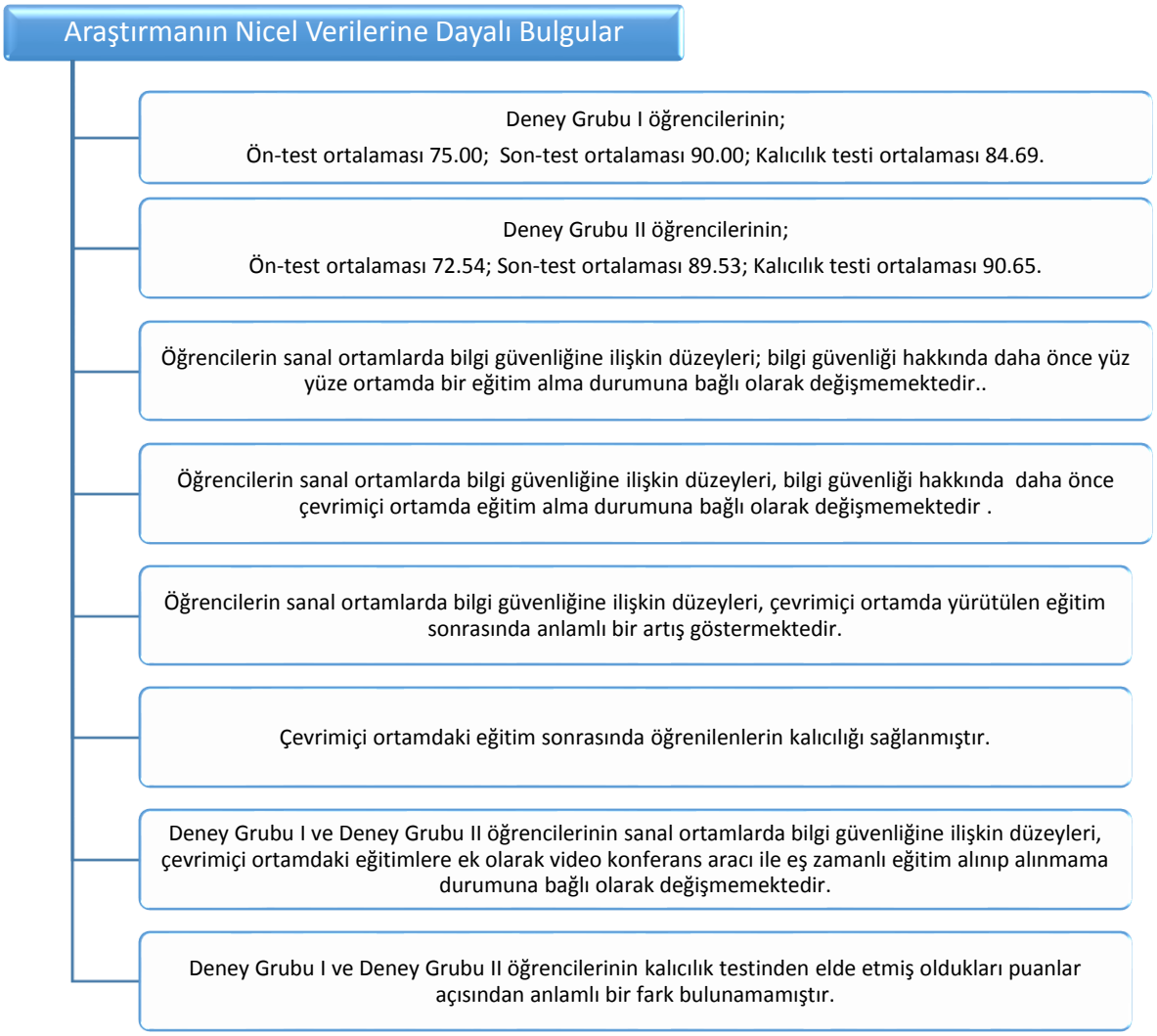
Deney Grubu II Öğrencilerinin Eş Zamanlı Derslerin Ne Gibi Katkılar Sağladığına Yönelik Görüşlerinin Dağılımı

Tema	%	f
Yeni bilgilerin öğrenilmesi	46,15	12
Konuların pekiştirilmesi	23,08	6
Eğitimin sürekliliğinin sağlanması.	23,08	6
Eksiklerin tamamlaması	3,85	1
Sitenin kullanımına yönelik destek alınabilmesi	3,85	1
Toplam Temaların Sayısı	**100,00**	**26**

Tablo 61 incelendiğinde, öğrencilerin tamamının eş zamanlı derslerin kendilerine katkı sağladığı görüşünde oldukları görülmektedir. Eş zamanlı derslerin ne gibi katkılar sağladığına yönelik olarak belirlenen temalar "Yeni bilgilerin öğrenilmesi, konuların pekiştirilmesi, eğitimin sürekliliğinin sağlanması, eksiklerin tamamlaması, sitenin kullanımına yönelik destek alınabilmesi" şeklindedir.

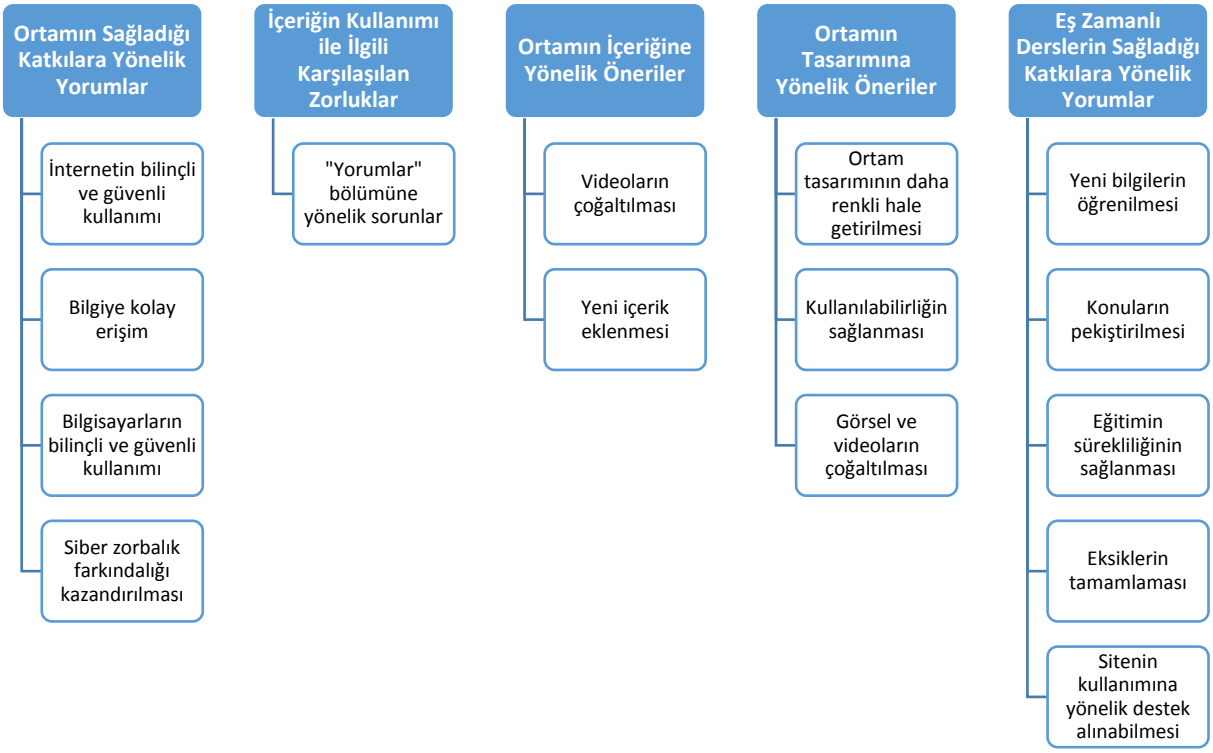
Çalışma Bulgularının Özeti

Bu çalışma kapsamında geliştirilen çevrimiçi ortamda alınan eğitimin öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerine etkisi araştırılmıştır. Bu amaç doğrultusunda nicel ve nitel verilerden faydalanılmıştır. Araştırmanın nicel verilerine dayalı olarak ulaşılan bulgular Şekil 9'da özetlenmiştir.



Şekil 9. Araştırmanın nicel verilerine dayalı bulgular

Sanal ortamlarda bilgi güvenliği ilgili olarak çevrimiçi ortamda yürütülen eğitimlere katılan öğrencilerin eğitim hakkındaki görüşlerine yönelik temalar Şekil 10'da özetlenmiştir.



Şekil 10. Çevrimiçi ortamda yürütülen eğitimlere katılan öğrencilerin eğitim hakkındaki görüşlerine yönelik temalar

Bölüm 5.
Sonuç, Tartışma ve Öneriler

Bu bölümde araştırma kapsamında ulaşılan sonuçlar ile ilgili araştırmalar bağlamında bu sonuçlarla ilgili olarak yapılan tartışmalar ve öneriler sunulmuştur.

Sonuç ve Tartışma

Bu araştırmada ulaşılan sonuçlar alt başlıklar halinde sunulmuştur. Araştırma kapsamında elde edilen nitel veriler, nicel verileri desteklemek amacıyla değerlendirilmiş ve tartışmaya dâhil edilmiştir.

Ortaokul öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri. Bu çalışmanın ilk araştırma sorusu, "*Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri nedir?"* şeklindedir. Bu soru doğrultusunda ulaşılan sonuçlara göre araştırmaya katılan iki farklı deney grubunun sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri denktir.

COVID-19 sürecinde, ağ teknolojilerinin iletişim, eğlence, iş, sağlık, eğitim ve oyun için kullanılmasıyla birlikte küçük çocukların ve ailelerin internet kullanımında birtakım değişiklikler ortaya çıkmıştır. Örneğin; ebeveynleri ve/veya aile üyeleri başka bir şekilde işle veya bakım görevleriyle meşgulken, zorunlu evde öğrenme dönemlerindeki tüm küçük çocukların çevrimiçi ortamda aktif olarak denetlenmediğine yönelik eksiklikler dikkat çekmiştir (Edwards, 2021). Avustralya'da, e-Güvenlik Ofisi, evde kalma emirlerini takiben küçük çocuklar tarafından internet tabanlı etkinliklerinin sürekli izlenmesi ihtiyacı konusunda ebeveynleri uyarmıştır (Office of eSafety Commissioner, 2020a).

Küçük çocukların siber güvenlik eğitimlerine olan ihtiyacı alanyazında sıklıkla dile getirilmekte ve vurgulanmaktadır (Office of eSafety Commissioner, 2020a; United Nations Committee on the Rights of Children, 2019). Bu tez çalışmasında, ortaokul öğrencilerinin çevrimiçi güvenlik ve risk ile ilgili eğitim alabilmesi amacıyla; alanyazın taraması doğrultusunda temalar belirlenerek, bir çevrimiçi eğitim ortamı tasarlanmıştır. Öğrenciler, tasarlanan bu ortamda yer alan eğitim ve etkinlikleri takip etmişlerdir. Bu kapsamda alınan eğitimin etkililiğine yönelik araştırma yapılmıştır.

Çocukların çevrimiçi mahremiyet anlayışlarının araştırıldığı bir çalışmanın sonuçlarında; çocukların özellikle çevrimiçi güvenlikle ilgili olduğunda, gizlilik konusunda bir anlayışa sahip oldukları ancak veriler ve hangi verilerin korunması gerektiği konusunda bazı yanılgılara sahip oldukları sonuçlarına ulaşılmıştır (Dempsey vd., 2018).

Alanyazında bilgi güvenliği, çevrimiçi güvenlik, çevrimiçi mahremiyet ve gizlilik gibi kavramlardan farklı olarak daha kapsayıcı olması sebebiyle "Siber sağlık" kavramı dikkat çekmektedir. Siber sağlık farkındalığı, uygun ve sorumlu teknoloji kullanımının yanı sıra internet kullanıcılarının korunmasına yönelik bilgi, beceri ve değerleri içermektedir (Mıhçı-Türker & Kılıç Çakmak, 2019). Araştırma sonuçları; öğrencilerin internet bağımlılığı, siber zorbalık, çevrimiçi mahremiyet ve siber güvenlik konusunda yüksek düzeyde farkındalığa, uygunsuz çevrimiçi içerik ve telif hakkı konusunda ise orta düzeyde farkındalığa sahip olduklarını göstermiştir (Mıhçı Türker ve Kılıç Çakmak, 2019). Bir başka çalışmada ise, sanal zorbalık davranışının; sanal aylaklık ve internet bağımlılığı ile pozitif, bilgi okuryazarlığı ile negatif yönde anlamlı bir ilişki oluşturduğu sonucuna ulaşılmış ve bu sonuç bilgi okuryazarlığı eğitiminin sanal zorbalığı ve diğer ilişkili sorunları önlemede önemli olduğu şeklinde yorumlanmıştır (Demir & Seferoğlu, 2016). Bahsedilen çalışmalardaki sonuçlara benzer bir biçimde, bu araştırma kapsamındaki sonuçlar bağlamında; öğrencilerin sanal ortamlarda bilgi güvenliği ile ilgili bir eğitim almadan önce bu konudaki farkındalıklarının ve bilgi düzeylerinin belirli bir seviyede olduğu ancak kapsamlı bir eğitimin daha fazla yarar sağlayacağı sonucuna ulaşılmıştır.

Ortaokul öğrencilerinin bilgi güvenliği hakkında daha önce yüz yüze ortamda ve çevrimiçi ortamda bir eğitim alma durumunun sanal ortamlarda bilgi güvenliğine ilişkin düzeylerine etkisi. Bu **ç**alışmanın ikinci araştırma sorusu "*Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri, öğrencilerin bilgi güvenliği hakkında daha önce yüz yüze ortamda bir eğitim alma durumuna göre nasıl değişmektedir?*" şeklindedir. Çalışmanın üçüncü araştırma sorusu ise "*Ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri, öğrencilerin bilgi güvenliği hakkında daha önce çevrimiçi ortamda bir eğitim alma durumuna göre nasıl değişmektedir?"* şeklindedir.

Bu araştırma sorularına yönelik olarak; öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin, bilgi güvenliği hakkında daha önce yüz yüze ya da

çevrimiçi bir eğitim alma durumuna bağlı olarak değişmediği sonucuna ulaşılmıştır. Bu sonucun, öğrencilerin daha önce katıldıklarını belirttikleri eğitimlerin kapsamının, çalışma kapsamında geliştirilen ortamda yer alan konulara kıyasla daha sınırlı olmasından kaynaklandığı düşünülebilir. Nitekim araştırmaya katılan öğrenciler beşinci sınıf düzeyinde, "Bilişim Teknolojileri ve Yazılım" dersi kapsamında çevrimiçi güvenlik ve risk ile ilgili olarak birtakım kazanımlara (Bkz. Tablo 37) yönelik eğitimler almışlardır (MEB Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı, 2018). Araştırma kapsamında geliştirilen çevrimiçi ortamda ise; kişisel verilerin korunması, sosyal ağların kullanımı, internet okuryazarlığı, siber zorbalık, çevrimiçi riskler, şifre güvenliği, zararlı yazılımlar, web güvenlik önlemleri ve güvenli olmayan iletişim yolları konularına yönelik kapsamlı bilgiler sunulmuş, "etkinlikler", "kendimizi sınayalım" ve "oyunlar" bölümleriyle konular pekiştirilerek eğitimler gerçekleştirilmiştir.

Avrupa Çevrimiçi Çocuklar (2020) projesi kapsamında; 19 ülkeden 7-17 yaş aralığındaki internet kullanıcıları ile gerçekleştirilen çalışmada; çevrimiçi ortamda kendini güvende hissetmenin, birçok çevrimiçi etkinliğe katılım için önemli bir faktör olduğu belirtilmiştir. Yine; dijital beceriler, çocukların internet aracılığıyla dünyayla başarılı bir şekilde bağlantı kurmasının temel bir ön koşul olarak vurgulanmaktadır (ITU, 2018). Öğrencilerin çevrimiçi ortamda kendilerini güvende hissetmesinin bir ön koşulu olarak dijital becerilerin; alınan eğitime ve yaşantılara bağlı olduğu düşünülebilir. Bu tez çalışmasında; öğrencilerin daha önce bilgi güvenliği ile ilgili bir eğitime katılma durumu göz önüne alınarak ve öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin bilgi düzeyleri açısından eşit seviyede oldukları belirlenerek eğitimlere başlanmıştır.

Sanal ortamlarda bilgi güvenliği ile ilgili eğitime yönelik tasarlanan ortamda yürütülen eğitimlerin ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliği ile ilgili bilgi durumlarındaki değişimine etkisi. Bu çalışmanın dördüncü araştırma sorusu "*Sanal ortamlarda bilgi güvenliği ile ilgili eğitime yönelik tasarlanan ortamda yürütülen eğitimlerin ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliği ile ilgili bilgi durumlarındaki değişimine etkisi nedir?*" şeklindedir. Bu araştırma sorusuna yönelik olarak, öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin tasarlanan ortamdaki eğitimler sonrasında yükseldiği sonucuna ulaşılmıştır. Bu durum, tasarlanan ortam aracılığıyla tamamen çevrimiçi ortamda

gerçekleştirilen eğitimin başarılı olduğu şeklinde yorumlanabilir. Öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzey belirleme aracına verdikleri yanıtlar incelendiğinde; öğrencilerin ön-testte verdikleri cevaplara kıyasla son-testte verdikleri cevaplarda, ilgili sorulara yönelik daha fazla kazanıma ulaştıkları belirlenmiştir. Örneğin internette etkili arama yapabilmek için kullanılabilecek yöntemlere ve siber zorbalık davranışına ilişkin kazanımların sınandığı sorulara yönelik, ön-testte öğrencilerin neredeyse tamamı ilgisiz yanıtlar verirken, son-testte öğrencilerin büyük çoğunluğunun, geliştirilen rubrik puanlama ölçütlerine uygun yanıtlar verdikleri belirlenmiştir.

Yetişkinlerin “siber tehdit eğitim seminerlerine” olan ilgisinin analiz edilmeye odaklanıldığı bir araştırma sonuçları, katılımcıların birçoğunun siber tehditler ve çocuklarının çevrimiçi alanı keşfetmesi konusunda endişeli olduğunu göstermiştir. Anket çalışmasında; katılımcılara siber tehditleri nasıl en aza indireceklerini ve en son gelişmeleri nasıl anlayacaklarını öğreten bir seminere katılmakla ilgilenip ilgilenmeyecekleri sorulmuş ve katılımcıların %80'inden fazlası siber güvenlik eğitimine katılma konusunda istekli olduklarını belirtmişlerdir (Ricci, 2019). Bahsedilen çalışmada görüldüğü üzere; çocukların çevrimiçi ortamlarda güvende olabilmesi ebeveynler açısından da oldukça önemsenmektedir.

Bovina vd. (2014) bilgi güvenliği kavramının çocuklar açısından anlamını araştırdıkları bir çalışma kapsamında elde ettikleri verilerde en sık kullanılan temaların bilgiye erişim, internet, sansür, kontrol, bilgi filtreleme, ebeveyn kontrolü ve yasaklar olduğunu tespit etmişlerdir. Bu araştırma kapsamında geliştirilen çevrimiçi ortamda yer alan temaların da Bovina vd.’nin çalışmalarında elde ettikleri temalarla örtüştüğünü söylemek mümkündür. Çocukların çevrimiçi güvenliğini başkalarının eylemlerine bağlı bir şey olarak görmenin yanı sıra çevrimiçi güvenlik çocukların bağımsızlıkları ve gelişimsel süreçleri ile etkinleşen bir eylem olarak da görülebilir (Hartikainen vd., 2019; Wisniewski vd., 2014). Bu anlamda çocukların çevrimiçi ortamdaki riskler konusunda da bilgi sahibi olmalarının önemli olduğu düşünülmektedir.

Çevrimiçi ortamlarda gizlilik konusuna yönelik yapılan bir çalışmada; 9-13 yaş arası çocuklara çevrimiçi mahremiyet-gizlilik okuryazarlığı eğitimi verilmiş; bu eğitimin çocukların çevrimiçi gizlilik okuryazarlığını nasıl artırabileceği ve çevrimiçi gizlilik davranışlarını nasıl etkileyebileceği araştırılmıştır. Gerçekleştirilen iki

çevrimiçi deney, eğitimin çocukların kişisel bilgileri saklama ve üretme dahil olmak üzere gizliliklerini daha iyi korumalarına ve çevrimiçi gizlilik anlayışını geliştirmelerine katkı sağladığını göstermiştir (Desimpelaere vd., 2020). Küçük çocuklar arasındaki ifşa davranışını araştıran bu çalışmada, mahremiyet-gizlilik okuryazarlığı eğitiminin çocukların paylaştığı doğru kişisel ayrıntıların sayısını azalttığı sonucuna ulaşılmıştır. Başka bir deyişle, mahremiyet okuryazarlığı eğitimini izleyen çocukların kişisel bilgileri uydurmak veya "paylaşma" düğmesine tıklayarak ifşa etmeyi reddetmek gibi mahremiyeti koruyan stratejilere daha fazla başvurdukları belirlenmiştir (Desimpelaere vd., 2020).

Dijital ayak izi ders tasarımının öğrencilerin dijital vatandaşlık konusundaki akademik başarılarına etkisinin incelendiği bir araştırmada; 5. ve 6. sınıf öğrencilerine yönelik çalışma yürütülmüştür. Araştırma sonuçları; öğrencilerin ön test ve son test puanları arasında anlamlı bir fark olduğunu göstermiştir. Başka bir deyişle, dijital ayak izi dersinin tasarımının dijital vatandaşlık konusundaki akademik başarı açısından olumlu bir etkisinin olduğu belirtilmiştir (Kuh Karyeli & Dağhan, 2019). Çocukların e-güvenlik becerilerini geliştirmek için etkileşimli bir web tabanlı öğrenme ortamının etkililiğini değerlendirmek amacıyla yürütülen bir araştırmanın sonuçları da çocukların e-güvenlik becerilerini geliştirmek için hem örgün eğitimde hem de yaygın öğrenme ortamlarında kullanılabilen web tabanlı öğrenme ortamının etkili olduğu şeklinde yorumlanmıştır (Nicolaidou & Venizelou, 2020).

Bahsedilen çalışmalardan elde edilen sonuçların; bu araştırma kapsamında elde edilen sonuçlarla da örtüştüğünü söylemek mümkündür. Bu çalışmada; öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin tasarlanan ortamdaki eğitimler sonrasında eğitim öncesindeki düzeylerine kıyasla çok daha yüksek olduğu belirlenmiştir. Çalışma kapsamında nitel verilerin sonuçları da nicel veriler aracılığıyla ulaşılan sonuçları destekleyecek kanıtlar sunmuştur. Örneğin; çevrimiçi öğrenme ortamının bilgi güvenliği açısından katkı sağladığı ve öğrencilerin büyük çoğunluğunun çevrimiçi öğrenme ortamında sunulan içeriğin kullanımı ile ilgili herhangi bir zorlukla karşılaşmadıkları sonucuna ulaşılmıştır. Bu sonuç, öğrencilerin aldıkları eğitim sonrasında sanal ortamlarda bilgi güvenliğine ilişkin bilgi düzeylerindeki artışı destekler nitelikte olarak yorumlanmıştır.

Çevrimiçi ortamda yürütülen çevrimiçi güvenlik ve risk ile ilgili eğitimlerin öğrenilenlerin kalıcılığına etkisi. Çalışmanın beşinci araştırma sorusu "*Çevrimiçi ortamda yürütülen bilgi güvenliği ile ilgili eğitimlerin öğrenilenlerin kalıcılığına etkisi nedir?*" şeklindedir. Bu araştırma sorusuna yönelik elde edilen veriler doğrultusunda; geliştirilen çevrimiçi ortamda yürütülen eğitimlerin öğrenilenlerin kalıcılığını sağlama konusunda etkili olduğu sonucuna ulaşılmıştır. Öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeyi belirleme aracına verdikleri yanıtlar incelendiğinde; öğrencilerin son-testte verdikleri cevaplar ve kalıcılık testinde verdikleri cevaplarda ilgili sorulara yönelik benzer kazanımlara ulaştıkları belirlenmiştir. Örneğin öğrencilerin verilen örnek senaryoda yer alan davranışı internette doğru ve güvenilir bilgiye erişim açısından değerlendirmelerinin hedeflendiği bir soruda, son-test ve kalıcılık testi cevapları bağlamında "sitenin güvenilirliğinin kontrol edilmesi ve bilginin doğruluğunun en az üç site incelenerek sorgulanması" temaları dikkat çekmektedir. Yine dijital bir oyun sitesinde tanışılan birisiyle iletişimde nasıl davranılması gerektiğine yönelik kazanımların hedeflendiği bir diğer soruda ise son-test ve kalıcılık testi cevapları bağlamında "cep telefonu bilgilerinin paylaşılmaması" temasının dikkat çektiği görülmektedir Bu yanıtlar bağlamında çevrimiçi ortamda yürütülen eğitimlerin bilginin transferi ve kalıcılığını sağladığı düşünülebilir.

Alanyazında öğrenilenlerin kalıcılığına yönelik gerçekleştirilen araştırmalarda da çalışma sonuçlarına benzer sonuçlarla karşılaşmak mümkündür. Örneğin lise düzeyinde "Temel Elektronik ve Ölçme" dersinde bilgisayar destekli zihin haritası kullanımının öğrenilenlerin kalıcılığı üzerindeki etkisini belirlemek amacıyla yapılan bir çalışmada; bilgisayar destekli zihin haritası kullanımının öğrenilenlerin kalıcılığını sağlamada etkili olduğu sonucuna ulaşılmıştır (Zeybek, 2020). Sınıf öğretmenlerinin eğitim aracı olarak interneti kullanma durumlarını betimlemenin amaçlandığı bir çalışmada, araştırma grubunda yer alan sınıf öğretmenlerinin tamamının öğretimin çeşitli süreçlerinde interneti kullandıkları ve ders hazırlıklarında en fazla faydalandıkları internet sitesinin egitimhane.com olduğu sonucuna ulaşılmıştır (Kula & Demirci- Güler, 2019). Çalışmada ayrıca sınıf öğretmenlerinin derste internet kullanımının bilgide kalıcılığı sağladığı yönünde bir görüşe sahip oldukları sonucuna ulaşılmıştır. Bu sonuç; bilginin farklı öğrenme materyalleri ile desteklenmesinin bilginin kalıcılığını sağlamada anlamlı etkisinin olduğu şeklinde yorumlanabilir.

Ortaokul öğrencilerinin eğitsel çevrim içi sosyal öğrenme ortamı Edmodo'nun erişiye ve kalıcılığa etkisinin araştırıldığı bir başka çalışma sonuçları da Edmodo ile zenginleşen öğrenme ortamının, öğrencilerin erişilerine olumlu etkisinin olduğunu, ayrıca öğrenmenin kalıcılığı bağlamında önemli bir katkı sağladığını göstermiştir (Bulca & Demirhan, 2020).

Bu tez çalışmasında; öğrencilerin sanal ortamlarda bilgi güvenliği ile ilgili bilgi edinmeleri ve bilginin kalıcılığının sağlanabilmesi amacıyla geliştirilen ortamda farklı materyaller ve etkinlikler sunulmuştur. Çalışma sonuçları iki farklı deney grubunda da uygulanan eğitimin bilginin kalıcılığını sağlamada etkili olduğunu göstermiştir. Elde edilen bu sonucun; alanyazındaki benzer çalışmaların sonuçlarıyla da tutarlılık gösterdiğini söylemek mümkündür.

Çevrimiçi ortamda eş zamansız eğitimlere katılan öğrenciler ile ilgili bilgi durumları ile eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliğine yönelik öğrenmeleri. Çalışmanın altıncı araştırma sorusu "*Çevrimiçi ortamda eş zamansız eğitimlere katılan ortaokul öğrencileri ile eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliğine yönelik öğrenmeleri açısından istatistiksel olarak anlamlı bir fark var mıdır?*" şeklindedir. Bu araştırma sorusuna yönelik olarak, çevrimiçi ortamda eş zamansız eğitimlere ek olarak gerçekleştirilen eş zamanlı eğitimlerin; sadece çevrimiçi ortamda gerçekleştirilen eş zamansız eğitimlere kıyasla öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri açısından bir farklılık oluşturmadığı sonucuna ulaşılmıştır.

Bu araştırmada; iki deney grubu öğrencilerinin ortalama puanlarının aldıkları eğitim sonrasında; sanal ortamlarda bilgi güvenliği düzeyleri açısından gruplar arasında anlamlı bir farklılık oluşturmadığı sonucuna ulaşılmıştır. Bu durumun; çevrimiçi ortamda eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin derse katılım düzeylerinden kaynaklandığı düşünülebilir. Öğrenciler COVID-19 küresel salgın sürecinde derslerin tamamını çevrimiçi ortamda aldıkları bir dönemde bu çalışmaya gönüllü katılım sağlamış, diğer derslerin sorumluluklarına ek olarak bu çalışmanın sorumluluklarını yerine getirmeye çalışmışlardır. Bu süreçte; eş zamanlı derslere katılımda aksaklıklar meydana gelebilmiştir.

Her ne kadar grupların puanları açısından anlamlı bir farklılık belirlenemese de, derslerin yürütülmesi sırasında birtakım farklılıklar gözlemlenmiştir. Eş zamanlı derslere katılan öğrencilerin geliştirilen çevrimiçi ortamdaki etkinlikleri gerçekleştirme konusunda diğer gruptaki öğrencilere kıyasla daha istekli oldukları gözlemlenmiştir. Örneğin; sadece çevrimiçi ortamdaki eş zamansız dersleri takip eden öğrenciler haftalık görevlerini gerçekleştirirken bazı konuları tamamlamayı unuttukları ve etkinlikleri yorumlamada zaman zaman zorlandıkları belirlenmiş; öğrencilerin velilerine hatırlatma yapılarak öğrencilerin konuları ve etkinlikleri tamamlanması sağlanmıştır. Çevrimiçi ortamdaki eş zamansız derslere ek olarak eş zamanlı derslere de katılan öğrencilerle iletişim daha güçlü olmuş; özellikle haftalık görevlerin tamamlanması süreci daha sağlıklı yürütülebilmiştir.

Ally (2008)'e göre eş zamansız çevrimiçi öğrenmede öğrenciler çevrimiçi malzemelere her zaman erişebilirken, eşzamanlı çevrimiçi öğrenme öğrenciler ve eğitmenler arasında gerçek zamanlı etkileşime izin verir. Eş zamanlı çevrimiçi sınıf oturumlarının yüz yüze iletişimin hala sanal alternatifinden daha etkili kabul edildiği günümüzde, yüz yüze iletişimin katılımcılar arasında daha yüksek düzeyde güven ve anlayış yaşanmasını sağladığı belirtilmektedir (Burdina vd., 2019). Bu doğrultuda eş zamanlı iletişim ve teknolojilerin kullanımının kısmen de olsa katılımcılar ve eğitmen arasındaki güven ve anlayışı sağlamada etkili olacağı düşünülebilir.

Bu araştırma kapsamında tasarlanan çevrimiçi ortamdaki materyallere öğrencilerin eş zamansız erişebilmelerinin bir avantaj sağladığı düşünülmektedir. Yine, eş zamanlı derslere katılan öğrenciler ve eğitmen arasındaki etkileşimin fazla olması beklenen bir sonuçtur. Bu araştırma kapsamında yürütülen uygulamalarda da, eğitmen-öğrenci etkileşiminin eş zamanlı dersler sonrasında diğer gruba kıyasla daha fazla olduğu gözlemlenmiştir. Eş zamanlı derslere katılan gruptaki öğrencilerin verilen görevleri daha kısa sürede tamamlama konusunda istekli olmalarının ve yine öğrenci velileriyle iletişimin kolay kurulabilmesinin de derslerdeki etkileşim sebebiyle gerçekleştiği söylenebilir.

Çevrimiçi ortamda eş zamansız eğitimlere katılan öğrenciler ile eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliği ile ilgili öğrendiklerinin kalıcılığı. Çalışmanın yedinci araştırma sorusu "*Çevrimiçi ortamda eş zamansız eğitimlere katılan öğrenciler ile eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin sanal*

ortamlarda bilgi güvenliğine yönelik öğrenilenlerin kalıcılığı açısından istatistiksel olarak anlamlı bir fark var mıdır?" şeklindedir. Bu araştırma sorusuna yönelik olarak, çevrimiçi ortamda eş zamansız eğitimlere katılan öğrenciler ile çevrimiçi ortamda eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrenciler arasında sanal ortamlarda bilgi güvenliğine ilişkin düzeylerinin kalıcılık puanları açısından bir farklılık oluşmadığı sonucuna ulaşılmıştır.

Mobil öğrenme bağlamında öğrencilerin öğrenmelerinin desteklenmesine katkı sağlamak amacıyla karekod uygulamasının erişi ve kalıcılık üzerindeki etkisinin incelendiği bir çalışmada; lise öğrencilerine yönelik bir araştırma gerçekleştirilmiştir. Deney grubu öğrencileri için kullanılan sunumlara karekodlar eklenmiş; ayrıca basılı olarak karekodlar öğrencilere dağıtılmıştır. Kontrol grubu öğrencileri için ise sunumların özetleri basılı olarak dağıtılmıştır. Araştırma sonuçlarına göre; kalıcılık açısından deney grubunun ortalama puanı kontrol grubunun ortalama puanına kıyasla daha yüksek olduğu, ancak gruplar arasında kalıcılık açısından anlamlı bir farklılık bulunamadığı belirtilmiştir (Akın, 2014).

Web tabanlı uzaktan eğitim ile geleneksel eğitimin başarıyı artırma ve kalıcılığı sağlama açısından karşılaştırılmasının yapıldığı bir çalışmada; İnternet Programcılığı 2 dersine katılan öğrencilere yönelik bir araştırma gerçekleştirilmiştir. Deney grubu öğrencileri Web Tabanlı Uzaktan Eğitim ortamında eğitim görürken, kontrol grubu ise Geleneksel Eğitim ortamında öğrenim görmüşlerdir. Çalışma sonuçları Web Tabanlı Uzaktan Eğitim'in başarıyı artırmada ve kalıcılığı sağlamada Geleneksel Eğitime göre daha başarılı olduğunu göstermiştir. Öğrencilerle yapılan görüşme sonuçlarına göre ise öğrencilerin Web Tabanlı Uzaktan Eğitime yönelik olarak pozitif düşüncelere sahip oldukları belirtilmiştir (Balaman, 2018). Geliştirilen bir mobil uygulamanın; öğrencilerin kimya dersi atom ve periyodik sistem ünitesindeki akademik başarılarına, kalıcı öğrenmelerine ve motivasyonlarına etkisinin araştırıldığı bir çalışmada ise; mobil uygulamayı kullanan öğrencilerin kalıcılık puanlarının uygulamayı kullanmayan öğrencilere göre daha yüksek olduğu tespit edilmiştir (Kılıç, 2015).

Alanyazında yer alan çalışmalardaki sonuçlar perspektifinde; çevrimiçi ortamda verilen eğitimlerin öğrenilenlerin kalıcılığını sağlaması konusunda etkili olacağını düşünmek mümkündür. Bu anlamda gerek sadece eş zamansız eğitimlere katılan gerekse eş zamansız eğitimlere ek olarak eş zamanlı etkinliklere katılan

gruplar açısından öğrenilenlerin kalıcı olduğu sonucuna ulaşılması beklenen bir sonuç olmuştur. Ancak; eş zamansız eğitimlere ek olarak eş zamanlı etkinliklere katılan öğrenciler açısından kalıcılık düzeyinin daha fazla olması beklenirken; grupların kalıcılık puanı açısından gruplar arasında anlamlı bir farklılık görülememiştir. Bu durum ise; çevrimiçi ortamda eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin derse katılım düzeyleri ile ilişkilendirilmiştir.

Sanal ortamlarda bilgi güvenliği ile ilgili olarak çevrimiçi ortamda yürütülen eğitimlere katılan öğrencilerin eğitime yönelik görüşleri. Çalışmanın sekizinci ve son araştırma sorusu "*Sanal ortamlarda bilgi güvenliği ile ilgili olarak çevrimiçi ortamda yürütülen eğitimlere katılan öğrencilerin aldıkları eğitime yönelik görüşleri nelerdir?*" şeklindedir. Bu çalışmaya katılan öğrencilerin büyük çoğunluğuna göre çevrimiçi öğrenme ortamı sanal ortamlarda bilgi güvenliğine ilişkin bilgi açısından katkı sağlamakta ve çevrimiçi öğrenme ortamında sunulan içeriğin kullanımı ile ilgili herhangi bir zorlukla karşılaşılmamaktadır.

Ortamın içeriğine yönelik olarak öğrencilerin büyük çoğunluğunun herhangi bir önerisi olmamıştır. Ortamın içeriğine yönelik öneriler kapsamında; "Videoların çoğaltılması" ve "Yeni içerik eklenmesi" önerileri dikkat çekmektedir. Ortamın tasarımına yönelik olarak da öğrencilerin büyük çoğunluğunun herhangi bir önerisi olmamıştır. Ortamın tasarımına yönelik öneriler kapsamında "ortam tasarımının daha renkli hale getirilmesi" ve "kullanılabilirliğin sağlanması" önerileri dikkat çekmektedir. Son araştırma sorusu kapsamında ayrıca öğrencilerin tamamının eş zamanlı derslerin kendilerine katkı sağladığı görüşünde oldukları sonucuna ulaşılmıştır. Eş zamanlı derslerin ne gibi katkılar sağladığına yönelik olarak "Yeni bilgilerin öğrenilmesi, konuların pekiştirilmesi, eğitimin sürekliliğinin sağlanması, eksiklerin tamamlaması, sitenin kullanımına yönelik destek alınabilmesi" temaları dikkat çekmektedir. Bu sonuç doğrultusunda çevrimiçi ortamlarda eş zamansız derslere ek olarak eş zamanlı derslerin yürütülmesinin, bilginin pekiştirilmesi ve öğretmenle daha iyi bir etkileşim sağlanabilmesi açısından katkı sağlayacağı söylenebilir

Öneriler

Bu bölümde araştırmaya yönelik öneriler, uygulamaya yönelik öneriler ve sanal ortamlarda bilgi güvenliği ile ilgili eğitimlerin sürdürülebilirliğine yönelik öneriler ayrı başlıklar halinde sunulmuştur.

Araştırmaya yönelik öneriler. Alanyazın incelendiğinde sanal ortamlarda bilgi güvenliği ile ilgili çevrimiçi ortamda gerçekleştirilen eğitimlerin etkililiğinin deneysel olarak araştırıldığı sınırlı sayıda çalışmaya rastlanmaktadır. Bu tez çalışması doğrultusunda deneysel desen kullanılarak ortaokul 6.sınıf öğrencilerine yönelik olarak sanal ortamlarda bilgi güvenliği ile ilgili çevrimiçi eğitimlerin etkililiği araştırılmıştır. Öğrencilerin ilkokul çağından itibaren çevrimiçi ortamları kullanmaları gerçeğinden hareketle özellikle ilkokul düzeyinde farklı yaş gruplarına yönelik olarak gerçekleştirilen çevrimiçi eğitimlerin etkililiğine yönelik yeni deneysel çalışmalar önerilebilir. Yine ortaokul düzeyinde bilgi güvenliğine ilişkin farkındalığın farklı yaş grupları ve sınıf kademeleri açısından artırılması önerilebilir.

Bu tez çalışmasının katılımcılarını, merkezi bir ortaokulda öğrenim görmekte olan 6. Sınıf öğrencileri oluşturmaktadır. Bu durum, araştırmanın genellenebilirliğinin benzer yaş düzeyindeki ortaokul öğrencileri açısından mümkün olduğu şeklinde yorumlanabilir. Dolayısıyla bu tez çalışması kapsamında yürütülen çalışmanın lise ve yükseköğretim öğrencilerine yönelik de gerçekleştirilmesi önerilmektedir.

Araştırma kapsamında çevrimiçi ortamda gerçekleştirilen sanal ortamlarda bilgi güvenliği eğitimlerinin, öğrencilerin bilgi güvenliği düzeyleri açısından anlamlı bir etkisinin olduğu belirlenmiştir. Bu durumun yanı sıra; tamamen yüz yüze ortamda yürütülen eğitimler ile tamamen çevrimiçi ortamda yürütülen eğitimlerin etkililiği açısından bir kıyaslama yapılması önerilebilir.

Bu tez çalışması kapsamında eş zamanlı ve eş zamansız tekniklerin kullanımının sanal ortamlarda bilgi güvenliğine ilişkin düzeylerine etkisine yönelik olarak bir araştırma yapılmıştır. Araştırma sonuçları doğrultusunda çevrimiçi ortamda eş zamansız eğitimlere katılan ortaokul öğrencileri ile çevrimiçi ortamda eş zamansız eğitimlere ek olarak eş zamanlı eğitimlere katılan öğrencilerin sanal ortamlarda bilgi güvenliği ile ilgili bilgi durumları ve öğrenilenlerin kalıcılığı açısından anlamlı bir fark bulunamamıştır. İleride yapılacak çalışmalar açısından eş zamanlı

derslere katılımın öğrencilere sağladığı katkılara yönelik nitel veriler doğrultusunda araştırmalar yapılması önerilebilir.

Uygulamaya yönelik öneriler. Alanyazında bilgi güvenliği ile ilgili eğitimlerin öğrencilerin farkındalığı ve davranışları açısından katkı sağladığına yönelik pek çok çalışmaya rastlanmaktadır. Bu tez çalışması, geliştirilen çevrimiçi ortamda verilen eğitimlerin sanal ortamlarda bilgi güvenliğine ilişkin bilgi açısından etkililiğini ortaya koymuştur. Dolayısıyla ilgili eğitimlerin çevrimiçi ortamda yürütülmesinin gerek zaman gerek eğitimlerin tekrarlanabilirliği, gerekse küresel salgın koşullarında eğitimin sürekliliğinin sağlanabilmesi açısından fayda sağladığı söylenebilir.

Bu çalışmada, bilgi güvenliği ile ilgili eğitimler öğrencilerin yaşları ve seviyeleri dikkate alınarak planlanmıştır. İleride yapılacak çalışmalar için, eğitimlerin yürütüleceği katılımcı kitlesinin ihtiyaçları ve seviyesi dikkate alınarak çevrimiçi ortamın içeriklerinin güncellenmesi önerilebilir. Eş zamanlı ve eş zamansız tekniklerin kullanıldığı bu deneysel çalışmada gerek sadece eş zamansız dersler gerekse eş zamansız derseler ek olarak gerçekleştirilen eş zamanlı derslerin öğrencilerin bilgi güvenliğine ilişkin düzeyleri açısından katkı sağladığı belirlenmiştir. Ayrıca; sadece eş zamansız derslere katılan öğrenciler ile eş zamansız derslere ek olarak eş zamanlı derslere de katılan öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri arasında anlamlı bir fark bulunamamıştır. Bu sonucun, küresel salgın koşullarında tamamen çevrimiçi ortamda eş zamanlı dersler aracılığıyla eğitimlere katılan öğrencilerin ders programlarının yoğunluğu ve motivasyon kaybından kaynaklandığı söylenebilir. Eğitimlerin tekrar yüz yüze gerçekleştirilmeye başlandığı şu günlerde; ileride yapılacak çalışmalar için eş zamansız ve eş zamanlı tekniklerin kullanımının etkililiğine yönelik tekrar bir inceleme yapılması önerilebilir.

Çalışma sonuçları geliştirilen çevrimiçi ortam aracılığıyla yürütülen eğitimlerin, öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin düzeyleri açısından etkili olduğunu göstermektedir. Yüz yüze eğitimin gerçekleştirilemediği ya da katılımcıların çevrimiçi eğitimi tercih ettiği durumlarda; bilgi güvenliği ile ilgili eğitimlerden daha fazla katılımcının yararlanması önerilebilir.

Sanal ortamlarda bilgi güvenliği ile ilgili çevrimiçi eğitimlerin sürdürülebilirliğine yönelik öneriler. Bilgi güvenliği ile ilgili çevrimiçi ortamda

yürütülecek eğitimlerde ders yürütücüsüne önemli sorumluluklar düşmektedir. Bu anlamda eğitimlerin sürekliliğinin sağlanmasına yönelik birtakım öneriler getirilmiştir.

Geliştirilen çevrimiçi ortamdaki derslere katılan öğrencilerin, katılım durumları haftalık olarak araştırmacı tarafından takip edilmiştir. Bu durum öğretmen- öğrenci etkileşimi açısından oldukça önemli olarak görülmektedir. Öğretmen-öğrenci etkileşimi geliştirilen ortam aracılığıyla katılımcı sayısının az olması sebebiyle sağlıklı bir şekilde yürütülebilmiştir. İleride yapılacak olan çalışmalarda daha fazla katılımcıyla çalışılması durumunda dersin yürütücüsünün her öğrenciyle kapsamlı bir etkileşim sağlayamayacağı göz önünde bulundurularak, eğitimlerin çok kalabalık gruplara yönelik olarak gerçekleştirilmemesi ya da daha az katılımcıdan oluşan birden fazla grupla yürütülmesi önerilmektedir.

Çevrimiçi ortamda yer alacak içeriklerin tasarlanması ciddi bir maliyet ve zaman gerektirdiğinden bu çalışmada hazır içeriklerden faydalanılmıştır. İleride yapılacak çalışmalara yönelik olarak birtakım içerik geliştirme çalışmalarının yapılması önerilebilir. Bununla birlikte içerik oluşturma ve oluşturulan içeriğin etkililiği ayrı bir araştırma konusu olarak düşünülebilir.

Genel bir özet yapmak gerekirse; bilgi güvenliği ile ilgili bir ortam tasarımının; öğrenci seviyesine uygun içerik seçimi, ortam tasarım süreci, geliştirilen ortamın kullanılabilirlik açısından değerlendirilmesi gibi aşamalar içerdiğini söylemek mümkündür. Araştırma sonuçları geliştirilen ortamda verilen eğitimlerin etkili bir şekilde uygulanabileceğini göstermektedir. Bu anlamda; öğretmen-öğrenci etkileşiminin yüksek seviyede tutulabileceği fazla kalabalık olmayan çalışma gruplarına yönelik olarak eğitimler planlanarak uygulamanın sürdürülebilirliğinin sağlanabileceği söylenebilir.

Kaynaklar

Ahn, J., Bivona, L. K., & Discala, J. (2011). Social media access in K12 schools: Intractable policy controversies in an evolving world. *Proceedings of the American Society for Information Science and Technology, 48*(1), 1-10.

Akın, T. (2014). Karekod destekli öğrenme materyalinin erişi ve kalıcılığa etkisi. (Yayımlanmamış yüksek lisans tezi). Hacettepe Üniversitesi, Eğitim Bilimleri Enstitüsü, Ankara.

Akpınar, Ş. (2019). *Blok tabanlı aktif öğrenme etkinlikleri ile basit elektrik devrelerinin öğretimi*. (Yayımlanmamış yüksek lisans tezi). Balıkesir Üniversitesi Fen Bilimleri Enstitüsü, Balıkesir.

Ally, M. (2004). Foundations of educational theory for online learning. *Theory and Practice of Online Learning*, 2, 15-44.

Ally, M. (2008). Role and function of theory in online education development and delivery. In T. Anderson (Eds.). The theory and practice of online learning, 45-74. (Second Edition), Athabasca: Athabasca University Press.

Anderson, T. (2008). Towards a theory of online learning. In T. Anderson (Eds.). *The Theory and practice of online learning*, 45-74. (Second Edition), Athabasca: Athabasca University Press.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34* (3), 613-643.

Arachchilage, N.A.G., Love S. (2014). Security awareness of computer users: a phishing threat avoidance perspective. *Computers in Human Behavior*. 38, 304–12.

Aslanyürek, M. (2016). İnternet ve sosyal medya kullanıcılarının internet güvenliği ve çevrimiçi gizlilik ile ilgili kanaatleri ve farkındalıkları. *Maltepe Üniversitesi İletişim Fakültesi Dergisi*, *3* (1), 80-106.

Balaman, F. (2018). Web tabanlı uzaktan eğitim ile geleneksel eğitimin İnternet Programcılığı 2 dersi kapsamında karşılaştırılması*. Itobiad: Journal of the Human & Social Science Researches, 7*(2). 1173-1200.

Balcı, B. (2010). E-öğrenme programı tasarım süreçleri. Türkiye'de e-öğrenme: Gelişmeler ve Uygulamalar içinde (83-110). Ankara, Cem Web Ofset.

Basham, J.D., Stahl, S., Ortiz, K., Rice, M.F., & Smith, S. (2015). *Equity Matters: Digital & Online Learning for Students with Disabilities*. Lawrence, KS: Center on Online Learning and Students with Disabilities.

Basham, J. D., Smith, S. J., & Satter, A. L. (2016). Universal design for learning: Scanning for alignment in K–12 blended and fully online learning materials. *Journal of Special Education Technology, 31*(3), 147-155.

Beder, A., & Ergün, E. (2015). Ortaokul öğrencilerinin güvenli internet kullanım durumlarının belirlenmesi. *Journal of Educational Sciences & Practices, 14*(27). 23-41.

Bilgi Teknolojileri ve İletişim Kurumu (2018). *Bilgi teknolojileri ve İnternetin bilinçli, güvenli kullanımı*. [Çevrimiçi: https://www.guvenliweb.org.tr/dosya/nH58Q.pdf, Erişim Tarihi: 20.05.2019].

Bovina, I. B., Dvoryanchikov, N. V., & Budykin, S. V. (2014). Shared meanings about information security of children: An exploratory study. *Procedia-Social and Behavioral Sciences, 146*, 94-98.

Boyd, D., & Hargittai, E. (2013). Connected and concerned: Variation in parents' online safety concerns. *Policy & Internet, 5*(3), 245-269.

Branon, R. F., & Essex, C. (2001). Synchronous and asynchronous communication tools in distance education. *TechTrends, 45*(1), 36-36.

Bulca, Y., & Demirhan, G. (2020). Eğitsel çevrimiçi sosyal öğrenme ortamı Edmodo'nun fiziksel aktivite kavramlarını öğrenmede erişiye ve kalıcılığa etkisi. *Eğitim Teknolojisi Kuram ve Uygulama, 10*(2), 577-589.

Burdina, G. M., Krapotkina, I. E., & Nasyrova, L. G. (2019). Distance learning in elementary school classrooms: An emerging framework for contemporary practice. *International Journal of Instruction, 12*(1), 1-16.

Büyüköztürk, Ş., Çakmak, E. K., Akgün, Ö. E., Karadeniz, Ş., ve Demirel, F. (2020). *Bilimsel araştırma yöntemleri* (28. Baskı). Ankara: Pegem Akademi.

Canbek, G., & Sağıroğlu, Ş. (2007). Çocukların ve gençlerin bilgisayar ve internet güvenliği. *Politeknik Dergisi, 10*(1).33-39.

Cassidy, S. (2004). Learning styles: An overview of theories, models, and measures. *Educational Psychology, 24*(4), 419-444.

Ceran, O., & Karataş, S. (*2021).* Development of an online learning system about information security, *Computers and Informatics, 1*(1), 26-35.

Chiong, R., & Jovanovic, J. (2012). Collaborative learning in online study groups: An evolutionary game theory perspective. *Journal of Information Technology Education: Research, 11*(1), 81-101.

Chui, L., Martin, K., & Pike, B. (2013). A quasi-experimental assessment of interactive student response systems on student confidence, effort, and course performance. *Journal of Accounting Education, 31*(1), 17-30.

Clarke, N., Symes, J., Saevanee, H., & Furnell, S. (2016). Awareness of Mobile Device Security: A Survey of User's Attitudes. *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, *7*(1), 15-31.

Common Sense Media. (n.d.). *Digital citizenship curriculum: Interactive lessons and activities for all students*. [Çevrimiçi: https://www.commonsense.org/education/digital-citizenship/curriculum?grades=3,4,5,6,7, Erişim Tarihi: 23.09.2021]

Çelen, F. K., Çelik, A., & Seferoğlu, S. S. (2011). Çocukların İnternet kullanımları ve onları bekleyen çevrim-içi riskler. XIII. *Akademik Bilişim Konferansı (AB11) Bildirileri*, 645-652. İnönü Üniversitesi, Malatya. [Çevrimiçi: http://ab.org.tr/ab11/kitap/celen_celik_Riskler_AB11.pdf, Erişim Tarihi: 10.11.2021]

Demir, Ö., & Seferoğlu, S. S. (2016). Bilgi okuryazarlığı, internet bağımlılığı, sanal aylaklık ve çeşitli diğer değişkenlerin sanal zorbalık ile ilişkisinin incelenmesi. *Online Journal of Technology Addiction and Cyberbullying, 3*(1), 1-26.

Dempsey, J., Sim, G., & Cassidy, B. (2018). Designing for GDPR-investigating children's understanding of privacy*:* A survey approach*. BCS Learning and Development Ltd. Proceedings of British HCI. Belfast, UK*

Design-Based Research Collective (2003). Design based research: An emerging paradigm for educational inquiry. *Educational Researcher, 32*(1), 5-8.

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior, 110*, 106382.

Dmitriev, S. M., Kononov, A. I., Shiriaev, M. V., & Malozemov, S. (2012). Cloud computing for education in state technical University of Nizhny Novgorod. *IFAC Proceedings Volumes, 45*(11), 418-420.

Edwards, S. (2021). Cyber-safety and COVID-19 in the early years: A research agenda. *Journal of Early Childhood Research*, *19*(3) 396–410.

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). *In Proceedings of the 33rd annual ACM conference on human factors in computing systems* (2873-2882).

Eren, S., & Erdem, M. (2020). Developing an Online environment scale for raising awareness of self-protection for the child*. Instructional Technology and Lifelong Learning, 1*(1), 63-87

Erol, S. R., & Sağıroğlu, Ş. (2018). Siber güvenlik farkındalığı, farkındalık ölçüm yöntem ve modelleri. *BGD Siber Güvenlik ve Savunma Kitap Serisi. Siber güvenlik ve savunma farkındalık ve caydırıcılık* (105-134). Grafiker Yayınları, Ankara.

Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2020). Youth internet safety education: Aligning programs with the evidence base. *Trauma, Violence, & Abuse*, 1-15.

Finkelhor, D., Jones, L., & Mitchell, K. (2021). Teaching privacy: A flawed strategy for children's online safety. *Child Abuse & Neglect*, *117*, 105064.

Gaffney, H., Farrington, D. P., Espelage, D. L., & Ttofi, M. M. (2019). Are cyberbullying intervention and prevention programs effective? A systematic and meta-analytical review. *Aggression and Violent Behavior,* 45, 134-153.

Gökçearslan, Ş., & Seferoğlu, S. S. (2016). Ortaokul öğrencilerinin internet kullanım biçimleri: Riskli davranışlar ve fırsatlar. *Kastamonu Eğitim Dergisi, 24*(1), 383-404.

Gunawardena, A. (2017). Brief survey of analytics in K12 and higher education. *International Journal on Innovations in Online Education*, *1*(1).

Gülbahar, Y. (2019). E-öğrenme'nin temelleri. *E-Öğrenme* içinde (2-18). Pegem Atıf İndeksi, 1-410. Ankara. 5.baskı.

Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *İlköğretim Online*, *15*(2).

Hadlington, L. J., & Chivers, S. (2018). *Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors.* Oxford: Oxford University Press. doi:10.1093/police/pay027.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16.

Harasim, L. (2000). Shift happens: Online education as a new paradigm in learning. *The Internet and Higher Education, 3*(1-2), 41-61.

Hartikainen, H., Livari, N., & Kinnula, M. (2019). Children's design recommendations for online safety education. *International Journal of Child-Computer Interaction, 22,* 100-146.

Hasebrink, U., Görzig, A., Haddon, L., Kalmus, V., & Livingstone, S. (2011). *Patterns of risk and safety online. In-depth analyses from the EU Kids Online survey of 9–16-year-olds and their parents in 25 countries.* LSE, London: EU Kids Online

International Computer Science Institute (2021). *Teaching privacy*. University of California Berkeley. [Çevrimiçi: https://teachingprivacy.org/, Erişim Tarihi: 23.09.2021]

ITU (2018). Measuring the Information Society Report Volume 2. [Çevrimiçi: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-2-E.pdf, Erişim Tarihi: 15.09.2021]

ITU (2020). International Telecommunication Union Definition of cybersecurity [Çevrimiçi: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx, Erişim Tarihi: 11.10.2020].

Jones, L. M., Mitchell, Kimberly J., & Walsh, W. A. (2014). *A content analysis of youth internet safety programs: Are effective prevention strategies being used?* Durham, NH: Crimes Against Children Research Center (CCRC), University of New Hampshire.

Kaşıkçı, D., Çağıltay, K., Karakuş, T., Kurşun, E., & Ogan, C. (2014). Türkiye ve Avrupa'daki çocukların internet alışkanlıkları ve güvenli internet kullanımı. *Eğitim ve Bilim, 39*(171), 230-243.

Karaoğlan Yılmaz, F. G., & Çavuş Ezin, Ç. (2017). Ebeveynlerin bilgi güvenliği farkındalıklarının incelenmesi. *Eğitim Teknolojisi Kuram ve Uygulama*, 7, 41-57.

Karaoğlan-Yılmaz, F. G., Yılmaz, R., & Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. *Bartın Üniversitesi Eğitim Fakültesi Dergisi, 3*(1), 176-199.

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, *61*, 46-58.

Keller, J. M. (1987). The systematic process of motivational design. *Performance+ Instruction, 26*(9-10), 1-8.

Khan, B. (1997). Web-based instruction: What is it and why is it? In B. H. Khan (Ed.), Web-based instruction (5–18). Englewood Cliffs, NJ: Educational Technology Publications.

Ki-Aries, D., & Faily, S. (2017). Persona-centered information security awareness. *Computers & Security*, 70, 663-674.

Kılıç, M. (2015). Mobil öğrenmeye dayalı Android uygulamalarının öğrencilerin Kimya dersi atom ve periyodik sistem ünitesindeki akademik başarılarına, kalıcı öğrenmelerine ve motivasyonlarına etkisi. (Yayımlanmamış yüksek lisans tezi). Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Kahramanmaraş.

Kılınç, D. (2012). Anayasal bir hak olarak kişisel verilerin korunması. *Ankara Üniversitesi Hukuk Fakültesi Dergisi, 61*(3), 1089-1172.

Kişisel Verileri Koruma Kurumu. (2016). *Kişisel Verilerin Korunması Kanunu (2016).* [Çevrimiçi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf, Erişim Tarihi: 18.05.2019].

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289-296.

Kuh Karyeli, G., & Dağhan, G. (2019). Sayısal ayak izi ders tasarımının öğrencilerin sayısal vatandaşlık konusundaki akademik başarılarına etkisi. *Erzincan Üniversitesi Eğitim Fakültesi Dergisi, 22*(1), 256-275.

Kula, S. S., & Demirci-Güler, M. P. (2019). Sınıf öğretmenlerinin interneti eğitim amaçlı kullanma durumları. *Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, *16*(1), 620-647.

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics, 33*, 159-174.

Lapitan Jr, L. D., Tiangco, C. E., Sumalinog, D. A. G., Sabarillo, N. S., & Diaz, J. M. (2021). An effective blended online teaching and learning strategy during the COVID-19 pandemic. *Education for Chemical Engineers*, *35*, 116-131.

Lindner, J., Clemons, C., Thoron, A., & Lindner, N. (2020). Remote instruction and distance education: A response to COVID-19. *Advancements in Agricultural development, 1*(2), 53-64.

Lilian, S. C. (2014). Virtual teams: Opportunities and challenges for e-leaders. *Procedia-Social and Behavioral Sciences,* 110, 1251-1261.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Technical Report and User Guide: The 2010 EU Kids Online Survey.* LSE, London: EU Kids Online.

Livingstone, S., & Smith, P.K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies, *J. Child Psychol. Psychiatr, 55*(6) 635–654, http://dx.doi.org/10.1111/jcpp.12197.

Mabrito, M. (2006). A study of synchronous versus asynchronous collaboration in an online business writing class. T*he American Journal of Distance Education, 20*(2), 93-107.

Magkos, E., Kleisiari, E., Chanias, P., & Giannakouris-Salalidis, V. (2014). Parental control and children's internet safety: The good, the bad and the ugly. *Proc. ICIL*, 18.

Means, B., Toyama, Y., Murphy, R., Bakia, M., & Jones, K. (2009). *Evaluation of evidence-based practices in online learning: A meta-analysis and review of online learning studies.* US Department of Education.

T.C. Millî Eğitim Bakanlığı (2018). Bilişim Teknolojileri ve Yazılım Dersi Öğretim Programı. [Çevrimiçi:https://mufredat.meb.gov.tr/Dosyalar/2018124103559587-Bili%C5%9Fim%20Teknolojileri%20ve%20Yaz%C4%B1l%C4%B1m%205-6.%20S%C4%B1n%C4%B1flar.pdf, Erişim Tarihi: 20.08.2021].

Mıhçı, P., & Kılıç Çakmak, E. (2017). Öğrenci siber sağlık ölçekleri geliştirme çalışması. *Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi, 37*(2), 457-491.

Mıhcı Türker, P., & 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.

Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. P*sychological Review, 63*(2), 81.

Moore, M. G. (1990). Background and overview of contemporary American distance education. Contemporary issues in American distance education (pp. xii−xxvi). NewYork: Pergamon Press.

Moore, M. (1997). Theory of transactional distance. *Theoretical Principles of Distance Education içinde 22-38*, Routledge.

Moore, J. L., Dickson-Deane, C., & Galyen, K. (2011). e-Learning, online learning, and distance learning environments: Are they the same? *The Internet and Higher Education, 14*(2), 129-135.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34, 47-66.

NICCS (National Initiative for Cybersecurity Careers and Studies). (2017). *Explore terms: A glossary of common cybersecurity terminology*. [Çevrimiçi: https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary#C,Erişim Tarihi: 08.09.2020].

Nicolaidou, I., & Venizelou, A. (2020). Improving children's E-safety skills through an interactive learning environment: A quasi-experimental study. *Multimodal Technologies and Interaction, 4*(2), 10.

Nielsen, J. (1993). *Usability engineering*. Boston, MA: Academic Press.

Office of eSafety Commissioner (2020a) COVID-19: An online safety kit for parents and carers. [Çevrimiçi: https://www.esafety.gov.au/about-us/blog/covid-19-online-safety-kit-parents-and-carers, Erişim Tarihi: 15.09.2021]

Office of the Privacy Commissioner of Canada. (n.d.). *Privacy and kids*. [Çevrimiçi: https://www.priv.gc.ca/en/privacy-topics/information-and-advice-for-individuals/privacy-and-kids/, Erişim Tarihi: 23.09.2021]

Ólafsson, K., Livingstone, S., & Haddon, L. (2013). *Children's use of online Technologies in Europe: A review of the European evidence base*. EU Kids Online. London, UK.

Padlipsky, S. (2018). Using *Offline Activities to Enhance Online Cybersecurity Education* (Unpublished master's theses). California Polytechnic State University, California.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117-129.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, 66, 40-51.

Paulsen, M. F. (2002). Online Education Systems: Discussion and definition of terms. *NKI Distance Education*, 202.

Power, M. (2009). *A designer's log: Case studies in instructional design*. [Çevrimiçi: https://www.aupress.ca/app/uploads/120161_99Z_Power_2009-Designers_Log.pdf, Erişim Tarihi: 13.05.2020.]

Raynes-Goldie, K., & Allen, M. (2014). Gaming Privacy: A Canadian case study of a children's co-created privacy literacy game. *Surveillance & Society, 12*(3), 414–426.

Reinholz, D. L., Stone-Johnstone, A., White, I., Sianez Jr, L. M., & Shah, N. (2020). A pandemic crash course: Learning to teach equitably in synchronous online classes. *CBE—Life Sciences Education, 19*(4), 1-13.

Rençber, Ö. F., & Mete, S. (2017). Bilgi güvenlik farkındalığını etkileyen faktörlerin belirlenmesi: Yüksek okul öğrencileri üzerine bir inceleme. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *18*(3), 800-823.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7-8), 241-253.

Rice, K. L. (2006). A comprehensive look at distance education in the K–12 context. *Journal of Research on Technology in Education*. *38*(4), 425-448.

Rice, M. F., & Carter Jr, R. A. (2015). When we talk about compliance, it's because we lived it": Online educators' roles in supporting students with disabilities. *Online Learning, 19*(5), 18-36.

Ricci, J., Breitinger, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies*, *24*(1), 231-249.

Roberts, T. S., & McInnerney, J. M. (2007). Seven problems of online group learning (and their solutions). *Journal of Educational Technology & Society, 10*(4), 257-268.

Rose, D. (2000). Universal design for learning. *Journal of Special Education Technology, 15*(3), 45-49.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

Sağıroğlu, Ş., & Alkan, M. (2018). *Siber güvenlik ve savunma farkındalık ve caydırıcılık*. *BGD Siber Güvenlik ve Savunma Kitap Serisi. s.26*. Grafiker Yayınları. Ankara.

Seferoğlu, S. S., Yıldız-Durak, H., Karaoğlan-Yılmaz, G., & Yılmaz, R. (2018). Bilgi güvenliği farkındalığı ve bilgi güvenliği politikalarıyla ilgili bir inceleme. B. Akkoyunlu, A. İşman & H. F. Odabaşı (Ed). *Eğitim teknolojileri okumaları 2018* (3. Bölüm, 29-43). TOJET ve Sakarya Üniversitesi, Adapazarı.

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, 199-207.

Siemens, G. (2005). *Connectivism: A learning theory for the digital age*. Çevrimiçi: http://www.itdl.org/journal/jan_05/article01.htm, Erişim Tarihi: 29.04.2019.

Skylar, A. A., Higgins, K., Boone, R., Jones, P., Pierce, T., & Gelfer, J. (2005). Distance education: An exploration of alternative methods and types of instructional media in teacher education. *Journal of Special Education Technology, 20*(3), 25-33.

Skylar, A. A. (2009). A comparison of asynchronous online text-based lectures and synchronous interactive web conferencing lectures*. Issues in Teacher Education, 18*(2), 69-84.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online. https://doi.org/10.21953/lse.47fdeqj01ofo

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.

Talan, T., Aktürk, C., Korkmaz, A., & Gülseçen, S. (2015). Üniversite öğrencilerinin akıllı telefon kullanımında güvenlik farkındalığı. *Istanbul Journal of Open and Distance Education*, *1*(2).

Talan, T., & Gülseçen, S. (2018). Ters-yüz sınıf ve harmanlanmış öğrenmede öğrencilerin öz-düzenleme becerilerinin ve öz-yeterlik algılarının incelenmesi. *Turkish Journal of Computer and Mathematics Education, 9*(3), 563-580.

Tekerek, M., & Tekerek, A. (2013). Öğrencilerin bilgi güvenliği farkındalığı üzerine bir araştırma. *Turkish Journal of Education, 2*(3), 61-70.

Tsim, S. J. (2006). *Internet safety education: information retention among middle school aged children*. (Unpublished master's theses). San Jose State University. California.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & Security,* 52, 128-141.

Tüzün, H. (2001). Guidelines for converting existing courses into web-based format. *Annual Proceedings of Selected Research and Development Papers Presented at the National Convention of the Association for Educational Communications and Technology*, 360-370, Atlanta.

United Nations Committee on the Rights of Children (2019). *General comment on the rights of children in digital environments*. [Çevrimiçi: https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx, Erişim Tarihi: 15.09.2021]

Wang, P., & Sbeit, R. (2017). A constructive team project model for online cybersecurity education*. Issues in Information Systems, 18*(3).

Wang, J., & Wang, Y. (2021). Compare synchronous and asynchronous online instruction for science teacher preparation. *Journal of Science Teacher Education, 32*(3), 265-285.

Wang, Q., Huang, C., & Quek, C. L. (2018). Students' perspectives on the design and implementation of a blended synchronous learning environment. *Australasian Journal of Educational Technology, 34*(1), 1-13.

Wankel, L., & Blessinger, P. (2012*). Increasing Student Engagement and Retention using Online Learning Activities*. Emerald Group Publishing: United Kingdom. ISBN 9781781902387.

Weiler, S. C. (2012). Quality virtual instruction: The use of synchronous online activities to engage international students in meaningful learning. *Journal of International Education and Leadership, 2*(2), 1-8.

Wei, H. C., & Chou, C. (2020). Online learning performance and satisfaction: do perceptions and readiness matter? *Distance Education, 41*(1), 48-69.

Wisniewski, P. J., Xu, H., Rosson, M. B., & Carroll, J. M. (2014, February). Adolescent online safety: The moral of the story. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*. 1258-1271). ACM.

Yıldırım, A., & Şimşek, H. (2011). *Sosyal bilimlerde nitel araştırma yöntemleri (8.Baskı).* Ankara: Seçkin Yayıncılık.

Zeybek, G. (2020). Bilgisayar destekli zihin haritası kullanımının akademik başarıya ve öğrenilenlerin kalıcılığına etkisi. *Electronic Journal of Education Sciences, 9*(18), 149-170.

Zilka, G. C. (2017). Awareness of eSafety and potential online dangers among children and teenagers. *Journal of Information Technology Education: Research,* 16, 319-338.

EK-A. Pilot Uygulamada Kullanılan Kişisel Bilgi Formu

Sayın ……..,

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu veri toplama sürecine katılım gönüllülük esasına dayalıdır. Araştırma ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerini geliştirebilmek amacıyla tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amaçlanmaktadır. Bu çalışmada ayrıca öğrencilerin bilgi güvenliği davranışlarına yönelik gelişimine ışık tutulacaktır. Çalışma Bilişim teknolojileri ve yazılım dersi müfredatına dayalı olarak yürütülecektir.

Bu formda vereceğiniz yanıtlar yalnızca araştırma amacıyla kullanılacak ve başkalarıyla paylaşılmayacaktır.

Katılımınız ve değerli katkınız için şimdiden çok teşekkür ederiz.

Fatma GÖLPEK SARI
Hacettepe Üniversitesi, Eğitim Bilimleri Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

Kişisel/Demografik Bilgiler

1.	**Cinsiyetiniz**	☐ Kadın ☐ Erkek

	Bir bilgisayara ve akıllı telefona sahiplik durumunuz:	Sahip Değilim.	1 Yıl.	2-5 Yıl.	6-10 Yıl ve Üzeri
2.	**Kendinize ait bir bilgisayarınız var mı?**	☐	☐	☐	☐
3.	**Kendinize ait bir akıllı telefonunuz var mı?**	☐	☐	☐	☐

	Çevrim-içi araçları kullanma sıklığınız	Hiçbir zaman	Nadiren	Ara sıra	Bazen	Her zaman
4.	**Dizüstü bilgisayar (Notebook, netbook, ultrabook vb.)**	☐	☐	☐	☐	☐

5.	**Masaüstü Bilgisayar**	☐	☐	☐	☐	☐
6.	**Tablet**	☐	☐	☐	☐	☐
7.	**Akıllı Telefon**	☐	☐	☐	☐	☐

8.	**Bilgisayar/İnternet kullanımınıza ilişkin günlük ortalama ayırdığınız süre**	☐ Hiç kullanmıyorum. ☐ 15 dakikadan az. ☐ 1 saatten az. ☐1-3 saat. ☐ 4-6 saat. ☐ 7 saat ve üzeri.

	İnterneti kullanım amaçlarınız nelerdir? Bu amaçlar amacıyla günlük ayırdığınız süre ne kadardır?	Hiç kullanmı yorum	15 dakika dan az	1 saatten az	1-3 saat	4-6 saat	7 saat ve üzeri
9.	**Haber okumak-medyayı takip etmek**	☐	☐	☐	☐	☐	☐
10.	**Eğlence amaçlı kullanmak**	☐	☐	☐	☐	☐	☐
11.	**Eğitim amacıyla kullanmak (araştırma yapmak, ödev yapmak, uzaktan eğitime devam etmek**	☐	☐	☐	☐	☐	☐

12.	**Bilgi güvenliği hakkında daha önce herhangi bir eğitim aldınız mı?**	☐ Evet ☐ Hayır

Formumuz burada sona ermiştir. Katıldığınız için çok teşekkür ederiz.

(Araştırma sonuçlarının sizinle paylaşılması için e-posta adresini bilgileriniz sadece sizinle araştırma sonuçlarını paylaşmak için istenilmektedir. Dilerseniz paylaşmayabilirsiniz.)

Formu yanıtlama işlemini sonlandırmak için "Gönder (Submit)" butonuna tıklayınız.

EK-B. Asıl Uygulamada Kullanılan Kişisel Bilgi Formu

Sevgili öğrenciler,

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu veri toplama sürecine katılım gönüllülük esasına dayalıdır. Araştırmada ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerini geliştirebilmek amacıyla tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amaçlanmaktadır. Bu çalışmada ayrıca öğrencilerin bilgi güvenliğine yönelik gelişimine ışık tutulacaktır. Çalışma Bilişim teknolojileri ve yazılım dersi müfredatına dayalı olarak yürütülecektir.

Bu formda vereceğiniz yanıtlar yalnızca araştırma amacıyla kullanılacak ve başkalarıyla paylaşılmayacaktır.

Katılımınız ve değerli katkınız için şimdiden çok teşekkür ederiz.

Fatma GÖLPEK SARI
Hacettepe Üniversitesi, Eğitim Bilimleri Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

1. İnterneti kullanım amaçlarınız ve bu amaçlar için günlük harcadığınız süre							
	Maddeler	Hiç kullanmıyorum	15 dakikadan az	15 dakika-1 saat	1-3 saat	4 -6 Saat	7 saat ve üzeri
a.	**Haber okumak- medyayı takip etmek**	☐	☐	☐	☐	☐	☐
b.	**Eğlence amaçlı kullanmak**	☐	☐	☐	☐	☐	☐
c.	**Eğitim amacıyla kullanmak (araştırma yapmak, ödev yapmak, uzaktan eğitime devam etmek**	☐	☐	☐	☐	☐	☐

2.	**Bilgi güvenliği hakkında daha önce yüz yüze ortamda eğitim alma durumunuz**	☐ Hiç eğitim almadım. ☐ Yüz yüze bir eğitime katıldım. ☐ Yüz yüze birkaç eğitime katıldım.

3.	**Bilgi güvenliği hakkında daha önce çevrimiçi ortamda eğitim alma durumunuz**	☐ Hiç eğitim almadım. ☐ Çevrimiçi bir eğitime katıldım. ☐ Çevrimiçi birkaç eğitime katıldım.

Formumuz burada sona ermiştir. Katıldığınız için çok teşekkür ederiz.

(Araştırma sonuçlarının sizinle paylaşılması için e-posta adresini bilgileriniz sadece sizinle araştırma sonuçlarını paylaşmak için istenilmektedir. Dilerseniz paylaşmayabilirsiniz.)

E-posta adresiniz:

Formu yanıtlama işlemini sonlandırmak için "Gönder (Submit)" butonuna tıklayınız.

EK-C. Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeyi Belirleme Aracı (Uzman Görüşleri Öncesi)

Sayın ……..,

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu veri toplama sürecine katılım gönüllülük esasına dayalıdır. Araştırmada ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerini geliştirebilmek amacıyla tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amaçlanmaktadır. Bu çalışma ayrıca öğrencilerin bilgi güvenliği davranışlarına yönelik gelişimine ışık tutulacaktır. Çalışma Bilişim Teknolojileri ve Yazılım dersi müfredatına dayalı olarak yürütülecektir.

Bu formda vereceğiniz yanıtlar yalnızca araştırma amacıyla kullanılacak ve başkalarıyla paylaşılmayacaktır.

Katılımınız ve değerli katkınız için şimdiden çok teşekkür ederiz.

Fatma GÖLPEK SARI
Hacettepe Üniversitesi, Eğitim Bilimleri Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

Soru 1. Kişisel veri kapsamına giren bilgilere bir örnek veriniz.

Soru 2. İnternette doğru ve güvenilir bilgiye ulaşabilmek için uygulanabilecek yöntemlerden bir tanesini yazınız.

Soru 3. Sosyal ağlarda bireylerin veri güvenliğine yönelik bazı riskler söz konusu olabilmektedir. Siz de sosyal ağlarda veri güvenliği açısından sorun oluşturabilecek bir durumu kısaca yazınız.

Soru 4. Siber zorbalık kavramını açıklayınız. Siber zorbalık davranışına bir örnek veriniz. Siber zorbalık davranışına maruz kalındığında neler yapılmalıdır, açıklayınız.

Soru 5. İnternette doğru ve etkili arama yapabilmek için kullanılabilecek yöntemlerden bir tanesini yazınız.

Soru 6. Güvenli şifre oluşturma yöntemlerine yönelik ölçütleri hatırlayarak, güvenli bir şifre örneği yazınız.

Soru 7. Güvenlik duvarı bilgisayarları hangi tehlikelerden korur ve hangi tehlikelerden korumaz? Güvenlik duvarı bilgisayarları korumak için yeterli bir önlem midir? Tartışınız.

Soru 8. Bir web sayfasında güvenli iletişim yolunun kullanılıp kullanılmadığı nasıl anlaşılır, anlatınız.

Soru 9. Bir siber zorbalık eylemiyle karşılaşmanız durumunda neler yapmanız gerekir? Bir örnekle açıklayınız.

Soru 10. Sosyal medyada hesap güvenliğine yönelik alınabilecek önlemlere bir örnek veriniz.

Soru 11. Aşağıda bir örnek senaryo verilmiştir. Bu senaryoda yer alan davranışı değerlendiriniz.
“Esra, öğretmeninin verdiği ödevle ilgili olarak internetten bir araştırma yapmıştır. Bu sırada Google arama motorunu kullanarak çıkan sonuçlardan ilk üçünü kullanmaya karar vermiş, bu üç web sayfasındaki içeriklerden kopyalayarak ve bazı kısımlarını da silerek ödevini hazırlamıştır.”

Soru 12. Siber zorbalık konusunda bir örnek oluşturup, bu örneğe uygun davranışın nasıl olması gerektiğine yönelik bir değerlendirme yapınız.

Soru 13. Aşağıda bir örnek senaryo verilmiştir:
“Emre, bir dijital oyun sitesinde birisiyle tanışmıştır. Bu kişi Emre’ye, oynadıkları oyun hakkında pratik bilgiler vermiş ve Emre’nin güvenini kazanmıştır. Bir süre sonra Emre’ye, eğer cep telefonu numarasını verirse ona oyuna dair bilgileri daha sık gönderebileceğini söyler.”
Bu durumda sizce Emre nasıl bir yol izlemelidir?

Soru 14. İnternette şifre güvenliğine yönelik neler yapabilirsiniz? Açıklayınız.

EK-Ç. Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeyi Belirleme Aracı (Uzman Görüşleri Sonrası)

Sayın ……..,

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu veri toplama sürecine katılım gönüllülük esasına dayalıdır Araştırmada ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerini geliştirebilmek amacıyla tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amaçlanmaktadır. Bu çalışmada ayrıca öğrencilerin bilgi güvenliği davranışlarına yönelik gelişimine ışık tutulacaktır. Çalışma Bilişim Teknolojileri ve Yazılım dersi müfredatına dayalı olarak yürütülecektir.

Bu formda vereceğiniz yanıtlar yalnızca araştırma amacıyla kullanılacak ve başkalarıyla paylaşılmayacaktır.

Katılımınız ve değerli katkınız için şimdiden çok teşekkür ederiz.

Fatma GÖLPEK SARI
Hacettepe Üniversitesi, Eğitim Bilimleri Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

Soru 1. Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Kişisel veri kapsamına giren bilgilere bir örnek veriniz.

Soru 2. İnternette doğru ve güvenilir bilgiye ulaşabilmek için uygulanabilecek yöntemlerden bir tanesini yazınız.

Soru 3. Sosyal ağlarda bireylerin veri güvenliğine yönelik siber zorbalık, kişisel bilgilerin paylaşımı ve kimlik hırsızlığı gibi bazı riskler söz konusu olabilmektedir. Sosyal ağlarda veri güvenliği açısından sorun oluşturabilecek bir durumu kısaca yazınız.

Soru 4. Siber zorbalık kavramını açıklayınız. Siber zorbalık davranışına bir örnek veriniz.

Soru 5. İnternette etkili arama yapabilmek için arama motorlarına yazacağımız açıklamalarda birtakım yöntemlere başvurabiliriz Bu yöntemlerden bir tanesini örnek vererek açıklayınız.

Soru 6. Güvenli şifre oluşturabilmek için kullanılması gereken yöntemlerden hareketle güvenli bir şifre örneği yazınız.

Soru 7. "Güvenlik duvarı; gelen ve giden ağ trafiğini kontrol ederek bilgisayarınıza ya da bilgisayar ağınıza yetkisiz veya istemediğiniz kişilerin çeşitli yollardan erişim sağlamasını engellemeye yarayan yazılımdır."
Güvenlik duvarı, bilgisayarları hangi tehlikelerden korur ve hangi tehlikelerden korumaz? Güvenlik duvarının bilgisayarları korumak için yeterli bir önlem olup olamayacağını açıklayınız.

Soru 8. Siber zorbalık eylemiyle karşılaşmanız durumunda neler yapmanız gerekir? Bir örnekle açıklayınız.

Soru 9. Sosyal medyada (Facebook, Whatsapp ,Twitter, Instagram vb.) hesap güvenliğimiz için alınabilecek önlemlerden bir tanesini örnekle açıklayınız.

Soru 10. Aşağıda bir örnek senaryo verilmiştir. Bu senaryoda yer alan davranışı internette doğru ve güvenilir bilgiye erişim açısından değerlendiriniz.
"Esra, öğretmeninin verdiği ödevle ilgili olarak internetten bir araştırma yapmıştır. Bu sırada arama motorunu kullanarak çıkan sonuçlardan ilk üçünü kullanmaya karar vermiş, bu üç web sayfasındaki içeriklerden kopyalayarak ve bazı kısımlarını da silerek ödevini hazırlamıştır."

Soru 11. Aşağıda bir örnek senaryo verilmiştir:
"Emre, bir dijital oyun sitesinde birisiyle tanışmıştır. Bu kişi Emre'ye, oynadıkları oyun hakkında pratik bilgiler vermiş ve Emre'nin güvenini kazanmıştır. Bir süre sonra Emre'ye, eğer cep telefonu numarasını kendisine verirse, ona oyuna dair bilgileri daha sık gönderebileceğini söyler."
Size göre Emre bu durumda nasıl bir yol izlemelidir?

EK-D. Sanal Ortamlarda Bilgi Güvenliğine İlişkin Düzeyi Belirleme Aracı ve Dereceli Puanlama Anahtarı

Sayın ……..,

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu veri toplama sürecine katılım gönüllülük esasına dayalıdır Araştırmada ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerini geliştirebilmek amacıyla tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amaçlanmaktadır. Bu çalışmada ayrıca öğrencilerin bilgi güvenliği davranışlarına yönelik gelişimine ışık tutulacaktır. Çalışma Bilişim Teknolojileri ve Yazılım dersi müfredatına dayalı olarak yürütülecektir.

Bu formda vereceğiniz yanıtlar yalnızca araştırma amacıyla kullanılacak ve başkalarıyla paylaşılmayacaktır.

Katılımınız ve değerli katkınız için şimdiden çok teşekkür ederiz.

Fatma GÖLPEK SARI
Hacettepe Üniversitesi, Eğitim Bilimleri Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı

Soru 1. Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Kişisel veri kapsamına giren bilgilere bir örnek veriniz.

SORU 1				**GÖRÜŞLERİNİZ**
Ölçütler	**Puanlamalar**			
	0 puan	**Kısmi Puan (5)**	**Tam Puan (10)**	
Kişisel veri kapsamına giren bilgilere bir örnek verilmesi	Örnek verilememiş veya hatalı örnek verilmiştir.	Örnek açık bir şekilde ifade edilmemiştir.	Örnek yeterince açık bir şekilde ifade edilmiştir.	

Soru 2. İnternette doğru ve güvenilir bilgiye ulaşabilmek için uygulanabilecek yöntemlerden bir tanesini yazınız.

SORU 2				**GÖRÜŞLERİNİZ**
Ölçütler	**Puanlamalar**			
	0 puan	**Kısmi Puan (5)**	**Tam Puan (10)**	
İnternette doğru ve güvenilir bilgiye ulaşabilmek için yöntemlere bir örnek verilmesi	Örnek verilememiş veya hatalı örnek verilmiştir.	Örnek açık bir şekilde ifade edilmemiştir.	Örnek yeterince açık bir şekilde ifade edilmiştir.	

Soru 3. Sosyal ağlarda bireylerin veri güvenliğine yönelik siber zorbalık, kişisel bilgilerin paylaşımı ve kimlik hırsızlığı gibi bazı riskler söz konusu olabilmektedir. Sosyal ağlarda veri güvenliği açısından sorun oluşturabilecek bir durumu kısaca yazınız.

SORU 3				**GÖRÜŞLERİNİZ**
Ölçütler	**Puanlamalar**			
	0 puan	**Kısmi Puan (5)**	**Tam Puan (10)**	
Paylaşıldığında kişileri zor durumda bırakabilecek bilgiler veya 3. Parti uygulamalara yönelik dikkat edilmesi gerekenlerden bahsedilmesi	Örnek verilememiş veya hatalı örnek verilmiştir.	Örnek açık bir şekilde ifade edilmemiştir.	Örnek yeterince açık bir şekilde ifade edilmiştir.	

Soru 4. Siber zorbalık kavramını açıklayınız. Siber zorbalık davranışına bir örnek veriniz.

SORU 4				**GÖRÜŞLERİNİZ**
Ölçütler	**Puanlamalar**			
	0 puan	**Kısmi Puan (2)**	**Tam Puan (4)**	
Siber zorbalık kavramının açıklanması	Kavrama yönelik açıklama yapılmamış veya ilgisiz bir açıklama yapılmış.	Kavram açık bir şekilde ifade edilmemiştir.	Kavram yeterince açık bir şekilde ifade edilmiştir.	
Siber zorbalık davranışına bir örnek verilmesi	Örnek verilememiş veya hatalı örnek verilmiştir.	Örnek açık bir şekilde ifade edilmemiştir.	Örnek yeterince açık bir şekilde ifade edilmiştir.	

Soru 5. İnternette etkili arama yapabilmek için arama motorlarına yazacağımız açıklamalarda birtakım yöntemlere başvurabiliriz Bu yöntemlerden bir tanesini örnek vererek açıklayınız.

SORU 5				**GÖRÜŞLERİNİZ**
Ölçütler	**Puanlamalar**			
	0 puan	**Kısmi Puan (5)**	**Tam Puan (10)**	
İnternette doğru ve etkili arama yapabilmek için kullanılabilecek yöntemlerin örneklendirilmesi	Örnek verilememiş veya hatalı örnek verilmiştir.	Örnek açık bir şekilde ifade edilmemiştir.	Örnek yeterince açık bir şekilde ifade edilmiştir.	

Soru 6. Güvenli şifre oluşturabilmek için kullanılması gereken yöntemlerden hareketle güvenli bir şifre örneği yazınız.

SORU 6			**GÖRÜŞLERİNİZ**
Ölçütler	**Puanlamalar**		
	0 puan	**Tam Puan (3)**	
En az 8 karakter kullanılmış olması	Bu ölçüt kullanılmamıştır.	Bu ölçüt kullanılmıştır.	
Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler içermesi	Bu ölçüt kullanılmamıştır.	Bu ölçüt kullanılmıştır.	
Büyük ve küçük harflerin bir arada kullanılması	Bu ölçüt kullanılmamıştır.	Bu ölçüt kullanılmıştır.	
Kişisel bilgiler gibi kolay tahmin edilebilecek bilgilerin kullanılmaması	Bu ölçüt kullanılmamıştır.	Bu ölçüt kullanılmıştır.	
Sözlükte bulunabilen kelimelerin kullanılmaması	Bu ölçüt kullanılmamıştır.	Bu ölçüt kullanılmıştır.	

Soru 7. “Güvenlik duvarı; gelen ve giden ağ trafiğini kontrol ederek bilgisayarınıza ya da bilgisayar ağınıza yetkisiz veya istemediğiniz kişilerin çeşitli yollardan erişim sağlamasını engellemeye yarayan yazılımdır.”

Güvenlik duvarı, bilgisayarları hangi tehlikelerden korur ve hangi tehlikelerden korumaz? Güvenlik duvarının bilgisayarları korumak için yeterli bir önlem olup olamayacağını açıklayınız.

SORU 7				**GÖRÜŞLERİNİZ**
Ölçütler	**Puanlamalar**			
	0 puan	**Kısmi Puan (2)**	**Tam Puan (4)**	
Güvenlik duvarının bilgisayarları hangi tehlikelerden koruduğuna yönelik açıklama yapılması	Cevap verilmemiş veya ilgisiz bir açıklama yapılmıştır.	İlgili cevaplar açık bir şekilde ifade edilmemiştir.	İlgili cevaplar yeterince açık bir şekilde ifade edilmiştir.	
Güvenlik duvarının bilgisayarları hangi tehlikelerden korumadığına yönelik bir açıklama yapılması	Cevap verilmemiş veya ilgisiz bir açıklama yapılmıştır.	İlgili cevaplar açık bir şekilde ifade edilmemiştir.	İlgili cevaplar yeterince açık bir şekilde ifade edilmiştir.	
Güvenlik duvarının bilgisayarları korumak yeterli olmadığına dair bir tartışma yürütülmesi.	Cevap verilmemiş veya ilgisiz bir açıklama yapılmıştır.	Tartışmaya yönelik yorum açık bir şekilde ifade edilmemiştir.	Tartışmaya yönelik yorum açık bir şekilde ifade edilmiştir.	

Soru 8. Siber zorbalık eylemiyle karşılaşmanız durumunda neler yapmanız gerekir? Bir örnekle açıklayınız.

SORU 8				**GÖRÜŞLERİNİZ**
Ölçütler	**Puanlamalar**			
	0 puan	**Kısmi Puan (5)**	**Tam Puan (10)**	
Bir siber zorbalık eylemiyle karşılaşılması durumunda neler yapılması gerektiğinin açıklanması	Örnek verilememiş veya hatalı örnek verilmiştir.	Örnek açık bir şekilde ifade edilmemiş veya eksik örnek verilmiştir.	Örnek yeterince açık bir şekilde ifade edilmiştir.	

Soru 9. Sosyal medyada (Facebook, Whatsapp ,Twitter, Instagram vb.) hesap güvenliğimiz için alınabilecek önlemlerden bir tanesini örnekle açıklayınız.

SORU 9				**GÖRÜŞLERİNİZ**
Ölçütler	**Puanlamalar**			
	0 puan	**Kısmi Puan (5)**	**Tam Puan (10)**	
Sosyal medyada hesap güvenliğine yönelik alınabilecek önlemlerin açıklanması	Örnek verilememiş veya hatalı örnek verilmiştir.	Örnek açık bir şekilde ifade edilmemiş veya eksik örnek verilmiştir.	Örnek yeterince açık bir şekilde ifade edilmiştir.	

Soru 10. Aşağıda bir örnek senaryo verilmiştir. Bu senaryoda yer alan davranışı internette doğru ve güvenilir bilgiye erişim açısından değerlendiriniz.
"Esra, öğretmeninin verdiği ödevle ilgili olarak internetten bir araştırma yapmıştır. Bu sırada arama motorunu kullanarak çıkan sonuçlardan ilk üçünü kullanmaya karar vermiş, bu üç web sayfasındaki içeriklerden kopyalayarak ve bazı kısımlarını da silerek ödevini hazırlamıştır."

SORU 10				**GÖRÜŞLERİNİZ**
Ölçütler	**Puanlamalar**			
	0 puan	**Kısmi Puan (5)**	**Tam Puan (10)**	
İnternette doğru ve güvenilir bilgiye ulaşma yolları referans gösterilerek açıklama yapılması	Cevap verilmemiş veya ilgisiz bir açıklama yapılmış.	İlgili cevaplar açık bir şekilde ifade edilmemiştir.	İlgili cevaplar yeterince açık bir şekilde ifade edilmiştir.	

Soru 11. Aşağıda bir örnek senaryo verilmiştir:
"Emre, bir dijital oyun sitesinde birisiyle tanışmıştır. Bu kişi Emre'ye, oynadıkları oyun hakkında pratik bilgiler vermiş ve Emre'nin güvenini kazanmıştır. Bir süre sonra Emre'ye, eğer cep telefonu numarasını kendisine verirse, ona oyuna dair bilgileri daha sık gönderebileceğini söyler."

Size göre Emre bu durumda nasıl bir yol izlemelidir?

SORU 11				**GÖRÜŞLERİNİZ**
Ölçütler	**Puanlamalar**			
	0 puan	Kısmi Puan (5)	Tam Puan (10)	
Sosyal ağlarda asla paylaşılmaması gereken bilgiler referans gösterilerek bir açıklama yapılması	Cevap verilmemiş veya ilgisiz bir açıklama yapılmış.	İlgili cevaplar açık bir şekilde ifade edilmemiştir.	İlgili cevaplar yeterince açık bir şekilde ifade edilmiştir.	

EK-E. Çevrimiçi Ortamın Değerlendirilmesine Yönelik Uzman Görüş Formu.

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Veri toplama sürecine katılımın gönüllülük esasına dayalı olduğu bu araştırmada ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerini geliştirebilmek amacıyla tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amaçlanmaktadır. Gerçekleştirilecek bu çalışmayla öğrencilerin, bilgi güvenliği davranışlarına yönelik gelişimine ışık tutulacaktır. Çalışma Bilişim teknolojileri ve Yazılım dersi müfredatına dayalı olarak yürütülecektir.

Sizlerden geliştirilen çevrimiçi ortamı incelemeniz, ortamı formda yer alan temalar doğrultusunda değerlendirmeniz beklenmektedir. Lütfen her bir tema için o temanın karşısında yer alan seçeneği/seçenekleri işaretleyiniz. Formda yer alan temalara ilişkin uyarı ve önerileriniz olursa "Temaya ilişkin uyarınız /öneriniz" sütunu altında bunları kısaca belirtiniz.

Ayırdığınız zaman ve değerli katkılarınız için şimdiden teşekkür ederim.

Bu formu, geri bildirimlerinizi ekledikten sonra (**fatmagolpek@gmail.com**) adresine yollayabilirsiniz.

Saygılarımla.

Fatma GÖLPEK SARI
Bilişim Teknolojileri Öğretmeni

Hacettepe Üniversitesi, Eğitim Bilimleri Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı
Doktora Öğrencisi

	Kullanılabilirlik İlkeleri	Uygun	Kısmen Uygun	Uygun Değil	Temaya İlişkin Uyarınız / Önerileriniz
1	**Öğrenilebilirlik**: Tasarımla, ortamı ilk kez kullanan kullanıcılar için temel görevleri gerçekleştirebilme kolaylığı				
2	**Verimlilik**: Tasarımın, kullanıcıların beklenen görevleri yapabilme hızı				
3	**Hatırlanabilirlik**: Tasarımın hatırlanabilir olması. Çevrimiçi öğrenme ortamını kullanmaya ara veren kullanıcıların geri döndüklerinde sistemi kullanmayı yeniden öğrenmek zorunda kalmaması				
4	**Hatalar**: Tasarımın, kullanıcıların yapabilecekleri/ karşılaşabilecekleri hataları önleyebilir ve yapılan hataların kolay telafi edilebilir olması.				
5	**Memnuniyet:** Tasarımın, kullanıcıyı memnun edecek yapıda, akıcı ve rahat olması.				

***Kullanılabilirlik ilkeleri Nielsen'dan (1993) uyarlanmıştır.**

Eğitim İçeriğini Değerlendirme Ölçütleri

Ünite	Konu	Hedeflenen Kazanımlar	Uygun	Kısmen Uygun	Uygun Değil	Temaya İlişkin Uyarınız/ Önerileriniz
1.Ünite: İnternetin Bilinçli Kullanımı	Kişisel Verilerin Korunması	Kişisel verinin ne anlama geldiğini bilir.				
		Veri sorumlusunun kim olduğunu, veri sorumlusunun görev ve sorumluluklarını bilir.				
		Kişisel verileri koruma kurumu ve kişisel verileri koruma kanunu hakkında bilgi edinir.				
		Kişisel verileri korumaya yönelik ne gibi önlemler alabileceğini öğrenir.				
1.Ünite: İnternetin Bilinçli Kullanımı	Sosyal Ağlar ve Mobil Ağlar	Sosyal ağlarda paylaşılmaması gereken bilgilerin farkına varır.				
		Sosyal ağlarda dikkat edilmesi gereken hususlar hakkında bilgi edinir.				
		Mobil ağlarda dikkat edilmesi gereken hususlar hakkında bilgi edinir.				
1.Ünite: İnternetin Bilinçli Kullanımı	İnternet Okuryazarlığı	İnternette etkili arama yöntemlerini bilir.				
		İnternet bilgi ağlarında yer alan bilgilerin doğrulunu sorgular.				
		İnternette doğru bilgiye ulaşma yollarını bilir.				
1.Ünite: İnternetin Bilinçli Kullanımı	Siber Zorbalık	Siber zorba ve siber mağdur kavramları hakkında bilgi edinir.				
		Hangi eylemlerin siber zorbalık kapsamına girdiğini bilir.				
		Siber zorbalıktan korunma yollarını bilir.				
		Siber zorbalığa maruz kaldığında ne yapacağın bilir.				
2.Ünite: İnternet ve Ağ Güvenliği	Şifre Güvenliği	Güçlü şifre oluşturma yöntemlerini bilir.				
2.Ünite: İnternet ve Ağ Güvenliği	Zararlı Yazılımlar	Bilgisayar virüsleri, truva atları, solucanlar ve casus yazılımlar hakkında bilgi edinir.				

Ünite	Konu	Hedeflenen Kazanımlar	Uygun	Kısmen Uygun	Uygun Değil	Temaya İlişkin Uyarınız/ Önerileriniz
		Bilgisayar virüsleri, truva atları, solucanlar ve casus yazılımların çalışma prensibini bilir.				
		Bilgisayar virüsleri, truva atları, solucanlar ve casus yazılımlardan korunma yollarını bilir.				
2.Ünite: İnternet ve Ağ Güvenliği	Web Tarayıcılarına Yönelik Güvenlik Önerileri	Web güvenliğiyle ilgili olarak tarayıcıları kullanırken alınabilecek güvenlik önlemlerini bilir.				
2.Ünite: İnternet ve Ağ Güvenliği	Güvenli Olmayan İletişim Yolları	İnternette kullanılan ve bilgi alışverişini sağlayan erişim protokolleri hakkında bilgi edinir.				
		Web sayfalarındaki güvenli iletişim yolu kullanımını anlayabilir.				

EK-F. Öğrencilerin Ortama İlişkin Görüşlerine Yönelik Açık Uçlu Anket Formu (Pilot Uygulama)

Sevgili öğrenciler,

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu veri toplama sürecine katılım gönüllülük esasına dayalıdır. Araştırmada ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerini geliştirebilmek amacıyla tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amaçlanmaktadır. Bilişim Teknolojileri ve Yazılım dersi müfredatına dayalı olarak yürütülecek olan bu çalışma öğrencilerin bilgi güvenliği davranışlarına yönelik gelişimine da katkı sağlayacaktır.

Bu formda vereceğiniz yanıtlar yalnızca araştırma amacıyla kullanılacak ve başkalarıyla paylaşılmayacaktır. Katılımınız ve değerli katkınız için şimdiden çok teşekkür ederiz.

Araştırma kapsamında kullanmış olduğunuz çevrimiçi öğrenme ortamının etkililiğinin belirlenebilmesi amacıyla aşağıdaki açık uçlu sorulardan oluşan formu doldurmanız beklenmektedir.

1. Sitenin ismi uygun mudur?
2. Sitede bulunan içerikler güncel midir?
3. Video ve anlatıların süresi ne kadar olmalıdır (daha uzun-kısa)?
4. "Kendimizi sınayalım" bölümü hakkında ne düşünüyorsun? Sana nasıl katkı sağladı?
5. "Etkinlikler" başlıklı bölümde yer alan etkinlikler hakkında ne düşünüyorsun? Bu etkinlikler ilgini çekti mi?
6. Sitenin en çok hangi yönünü beğendin?
7. Sitenin en az hangi yönünü beğendin?
8. Bu site sana bilgi güvenliği hakkında ne gibi katkılar sağladı?
9. Web sitesini kullandığın süreçte ne tür zorluklarla karşılaştın?
10. Öğrencilere yönelik bir bilgi güvenliği eğitiminde sence başka hangi konulara yer verilmelidir?

11. Uygulamada yer alan “Yeni Yorum Ekle” bölümünde diğer kullanıcılarla gerçekleştirilen iletişimin öğrenmene ne gibi katkılar sağladığını düşünüyorsun?

Not: Araştırmacının gönüllü öğrencilerle yapacağı görüşmelerde soracağı yukarıdaki sorular “ÖĞRENCİ GÖNÜLLÜ KATILIM FORMU (NİTEL)” başlıklı formla birlikte kullanılacaktır.

EK-G. Asıl Uygulamada Kullanılan Açık Uçlu Anket Formu (Deney Grubu I)

Sevgili öğrenciler,

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu veri toplama sürecine katılım gönüllülük esasına dayalıdır. Araştırmada ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerini geliştirebilmek amacıyla tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amaçlanmaktadır. Bilişim Teknolojileri ve Yazılım dersi müfredatına dayalı olarak yürütülecek olan bu çalışma öğrencilerin bilgi güvenliği davranışlarının gelişimine da katkı sağlayacaktır.

Bu formda vereceğiniz yanıtlar yalnızca araştırma amacıyla kullanılacak ve başkalarıyla paylaşılmayacaktır. Katılımınız ve değerli katkınız için şimdiden çok teşekkür ederiz.

Araştırma kapsamında kullanmış olduğunuz çevrimiçi öğrenme ortamının etkililiğinin belirlenebilmesi amacıyla aşağıdaki açık uçlu sorulardan oluşan formu doldurmanız beklenmektedir.

Soru 1. Çevrimiçi öğrenme ortamının size bilgi güvenliği açısından ne gibi katkılar sağladığını düşünüyorsunuz? Eğer katkı sağlamadığını düşünüyorsanız bu durumu nasıl açıklarsınız?

Soru 2. Çevrimiçi öğrenme ortamını kullandığınız süreçte içeriği kullanmak ve yorumlamak ilgili ne gibi zorluklarla karşılaştınız?

Soru 3. Kullandığınız ortamın içeriğine yönelik önerileriniz nelerdir?

Soru 4. Kullandığınız ortamın tasarımına yönelik önerileriniz nelerdir?

EK-Ğ. Asıl Uygulamada Kullanılan Açık Uçlu Anket Formu (Deney Grubu II)

Sevgili öğrenciler,

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu veri toplama sürecine katılım gönüllülük esasına dayalıdır. Araştırmada ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerini geliştirebilmek amacıyla tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amaçlanmaktadır. Bilişim Teknolojileri ve Yazılım dersi müfredatına dayalı olarak yürütülecek olan bu çalışma öğrencilerin bilgi güvenliği davranışlarının gelişimine da katkı sağlayacaktır.

Bu formda vereceğiniz yanıtlar yalnızca araştırma amacıyla kullanılacak ve başkalarıyla paylaşılmayacaktır. Katılımınız ve değerli katkınız için şimdiden çok teşekkür ederiz.

Araştırma kapsamında kullanmış olduğunuz çevrimiçi öğrenme ortamının etkililiğinin belirlenebilmesi amacıyla aşağıdaki açık uçlu sorulardan oluşan formu doldurmanız beklenmektedir.

Soru 1. Çevrimiçi öğrenme ortamının size bilgi güvenliği açısından ne gibi katkılar sağladığını düşünüyorsunuz? Eğer katkı sağlamadığını düşünüyorsanız bu durumu nasıl açıklarsınız?

Soru 2. Çevrimiçi öğrenme ortamını kullandığınız süreçte içeriği kullanmak ve yorumlamak ilgili ne gibi zorluklarla karşılaştınız?

Soru 3. Kullandığınız ortamın içeriğine yönelik önerileriniz nelerdir?

Soru 4. Kullandığınız ortamın tasarımına yönelik önerileriniz nelerdir?

Soru 5. Video konferans aracını kullanarak katıldığınız canlı dersler size ne gibi katkılar sağladı?

EK-H. Pilot Çalışmaya Katılan Öğrencilerin Ön-Test Sonuçları

Sıra	Alınan Puanlar
1	65
2	60
3	73
4	92
5	77
6	55
7	59
8	53
9	81
10	90
11	12
12	36
13	82
14	49
15	47
16	72
17	54
18	56
19	70
20	63
21	57
22	90
23	56
24	64
25	64
26	91
27	68
28	83
29	83
30	44

EK-I. Pilot Çalışmaya Katılan Öğrencilerin Son-Test Sonuçları

Sıra	Alınan Puanlar
1	86
2	95
3	69
4	110
5	95
6	100
7	93
8	87
9	85
10	115
11	76
12	72
13	105
14	64
15	72
16	104
17	97
18	85
19	92
20	90
21	93
22	115
23	105
24	71
25	74
26	77
27	99
28	106
29	111
30	111

EK-İ. Pilot Çalışmaya Katılan Öğrencilerin Kalıcılık Testi Sonuçları

Sıra	Alınan Puanlar
1	86
2	72
3	78
4	89
5	93
6	76
7	81
8	101
9	88
10	115
11	86
12	96
13	95
14	45
15	70
16	109
17	83
18	83
19	85
20	82
21	81
22	104
23	101
24	67
25	83
26	79
27	100
28	107
29	97
30	86

EK-J. Asıl Uygulamaya Katılan Deney Grubu I Öğrencilerinin Ön-Test Sonuçları

Sıra	Alınan Puanlar
1	75
2	74
3	93
4	63
5	78
6	90
7	24
8	77
9	60
10	84
11	81
12	89
13	82
14	107
15	64
16	90
17	73
18	78
19	75
20	75
21	73
22	64
23	72
24	56
25	56
26	97

EK-K. Asıl Uygulamaya Katılan Deney Grubu II Öğrencilerinin Ön-Test Sonuçları

Sıra	Alınan Puanlar
1	89
2	79
3	82
4	93
5	47
6	33
7	86
8	87
9	21
10	68
11	77
12	63
13	73
14	84
15	72
16	85
17	94
18	83
19	69
20	87
21	87
22	73
23	38
24	59
25	85
26	72

EK-L. Asıl Uygulamaya Katılan Deney Grubu I Öğrencilerinin Son-Test Sonuçları

Sıra	Alınan Puanlar
1	106
2	78
3	111
4	100
5	96
6	92
7	69
8	100
9	60
10	89
11	72
12	106
13	94
14	107
15	96
16	84
17	82
18	80
19	97
20	86
21	74
22	65
23	97
24	90
25	104
26	105

EK-M. Asıl Uygulamaya Katılan Deney Grubu II Öğrencilerinin Son-Test Sonuçları

Sıra	Alınan Puanlar
1	101
2	102
3	81
4	108
5	89
6	68
7	102
8	64
9	59
10	115
11	108
12	91
13	79
14	90
15	111
16	84
17	104
18	110
19	70
20	99
21	79
22	105
23	53
24	72
25	115
26	69

EK-N. Asıl Uygulamaya Katılan Deney Grubu I Öğrencilerinin Kalıcılık Testi Sonuçları

Sıra	Alınan Puanlar
1	82
2	86
3	82
4	82
5	82
6	104
7	69
8	99
9	53
10	100
11	97
12	79
13	78
14	109
15	105
16	84
17	90
18	74
19	78
20	78
21	52
22	76
23	97
24	84
25	82
26	100

EK-O. Asıl Uygulamaya Katılan Deney Grubu II Öğrencilerinin Kalıcılık Testi Sonuçları

Sıra	Alınan Puanlar
1	97
2	107
3	65
4	115
5	98
6	102
7	96
8	100
9	54
10	115
11	112
12	98
13	79
14	105
15	111
16	78
17	86
18	97
19	88
20	90
21	97
22	95
23	41
24	72
25	102
26	57

EK-Ö. Öğrenci Gönüllü Katılım Formu (Nicel)

__.__.20__

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu araştırma ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine yönelik tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amacını taşımaktadır. Bu çalışma ayrıca öğrencilerin bilgi güvenliği davranışlarına yönelik gelişimine ışık tutulacaktır. Çalışma Bilişim teknolojileri ve yazılım dersi müfredatına dayalı olarak yürütülecektir.

Bu çalışmada sizden çevrimiçi ortamdaki eğitime katılım göstermeniz ve birtakım soruları yanıtlamanız beklenmektedir. Bu çalışma sürecinde katılım gönüllülük esasına dayalıdır. Bu nedenle isterseniz çalışmaya katılmayabilirsiniz veya doldurmuş olduğunuz verinin silinmesini talep edebilirsiniz. Bu istek hemen yerine getirilecek ve sizin için herhangi bir olumsuzluk doğurmayacaktır. Araştırma için Milli Eğitim Bakanlığı'ndan gerekli izinler alınmıştır. Bu araştırma için ayrıca "Hacettepe Üniversitesi Etik Komisyonundan" da izin alınmıştır. Çalışmada toplanan veriler sadece çalışmada ismi geçen araştırmacılar tarafından incelenecek ve üçüncü kişilerle asla paylaşılmayacaktır. Çalışma bittikten sonra araştırmacılardan çalışmanın sonuçları hakkında bilgi alabilirsiniz. Bu sonuçlar ve aklınıza gelen herhangi bir başka soru için aşağıda bulunan e-posta aracılığıyla araştırmacılar ile çekinmeden iletişime geçebilirsiniz.

Yukarıda yazılanları okudum ve bahsedilen çalışmaya tamamen kendi isteğim ile katılmayı kabul ediyorum.

Katılımcı:	
Adı Soyadı:	
Tarih:	
İmza:	

Araştırmacı:		**Danışman:**	
Adı ve Soyadı:	Fatma GÖLPEK SARI	***Adı ve Soyadı:***	Prof. Dr. Süleyman Sadi SEFEROĞLU
Adres:	Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü	***Adres:***	Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Tarih:		***Tarih:***	
İmza:		***İmza:***	

EK-P. Öğrenci Gönüllü Katılım Formu (Nitel)

__.__.20__

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu araştırma ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine yönelik tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amacını taşımaktadır. Bu çalışma ayrıca öğrencilerin bilgi güvenliği davranışlarına yönelik gelişimine ışık tutulacaktır. Çalışma Bilişim teknolojileri ve yazılım dersi müfredatına dayalı olarak yürütülecektir.

Bu çalışmada sizden görüşlerinizi alabileceğimiz birtakım formları doldurmanızı bekleyeceğiz. Bu çalışma sürecinde katılım gönüllülük esasına dayalıdır. Bu nedenle isterseniz çalışmaya katılmayabilirsiniz veya doldurmuş olduğunuz verinin silinmesini talep edebilirsiniz. Bu istek hemen yerine getirilecek ve sizin için herhangi bir olumsuzluk doğurmayacaktır. Bu araştırma için Milli Eğitim Bakanlığı'ndan gerekli izinler alınmıştır. Araştırma için ayrıca "Hacettepe Üniversitesi Etik Komisyonundan" da izin alınmıştır. Çalışmada toplanan veriler sadece çalışmada ismi geçen araştırmacılar tarafından incelenecek ve üçüncü kişilerle asla paylaşılmayacaktır. Çalışma bittikten sonra araştırmacılardan çalışmanın sonuçları hakkında bilgi alabilirsiniz. Bu sonuçlar ve aklınıza gelen herhangi bir başka soru için aşağıda bulunan e-posta aracılığıyla araştırmacılar ile çekinmeden iletişime geçebilirsiniz.

Yukarıda yazılanları okudum ve bahsedilen çalışmaya tamamen kendi isteğim ile katılmayı kabul ediyorum.

Katılımcı:	
Adı Soyadı:	
Tarih:	
İmza:	

Araştırmacı:		**Danışman:**	
Adı ve Soyadı:	Fatma GÖLPEK SARI	***Adı ve Soyadı:***	Prof. Dr. Süleyman Sadi SEFEROĞLU
Adres:	Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü	***Adres:***	Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Tarih:		***Tarih:***	
İmza:		***İmza:***	

EK-R. Veli Gönüllü Katılım Formu (Nicel)

__.__.20__

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu araştırma ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine yönelik tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amacını taşımaktadır. Bu çalışma ayrıca öğrencilerin bilgi güvenliği davranışlarına yönelik gelişimine ışık tutulacaktır. Çalışma Bilişim teknolojileri ve yazılım dersi müfredatına dayalı olarak yürütülecektir.

Bu çalışmada velisi bulunduğunuz öğrencimizin birtakım soruları yanıtlaması beklenmektedir. Bu çalışma sürecine katılım gönüllülük esasına dayalıdır. Bu nedenle isterseniz öğrencimiz çalışmaya katılmayabilir veya doldurmuş olduğu verinin silinmesini talep edebilir, edebilirsiniz. Bu istek hemen yerine getirilecek, siz ve öğrencimiz için herhangi bir olumsuzluk doğurmayacaktır. Bu araştırma için Milli Eğitim Bakanlığı'ndan gerekli izinler alınmıştır. Araştırma için ayrıca "Hacettepe Üniversitesi Etik Komisyonundan" da izin alınmıştır. Çalışmada toplanan veriler sadece çalışmada ismi geçen araştırmacılar tarafından incelenecek ve üçüncü kişilerle asla paylaşılmayacaktır. Çalışma bittikten sonra araştırmacılardan çalışmanın sonuçları hakkında bilgi alabilirsiniz. Bu sonuçlar ve aklınıza gelen herhangi bir başka soru için aşağıda bulunan e-posta aracılığıyla araştırmacılar ile çekinmeden iletişime geçebilirsiniz.

Yukarıda yazılanları okudum ve bahsedilen çalışmaya velisi bulunduğum …….. 'nın tamamen kendi isteğimiz ile katılmasını kabul ediyorum.

Katılımcı:	
Adı Soyadı:	
Tarih:	
İmza:	

Araştırmacı:		**Danışman:**	
Adı ve Soyadı:	Fatma GÖLPEK SARI	***Adı ve Soyadı:***	Prof. Dr. Süleyman Sadi SEFEROĞLU
Adres:	Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü	***Adres:***	Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Tarih:		***Tarih:***	
İmza:		***İmza:***	

EK-S. Veli Gönüllü Katılım Formu (Nitel)

__.__.20__

Bu formun amacı Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Prof. Dr. Süleyman Sadi SEFEROĞLU'nun danışmanlığında yapılan doktora tezi kapsamında gerçekleştirilen bir araştırmaya veri toplamaktır. Bu araştırma ortaokul öğrencilerinin sanal ortamlarda bilgi güvenliğine yönelik tasarlanan ortamda yürütülen eğitimlerin verimliliğinin incelenmesi amacını taşımaktadır. Bu çalışma ayrıca öğrencilerin bilgi güvenliği davranışlarına yönelik gelişimine ışık tutulacaktır. Çalışma Bilişim teknolojileri ve yazılım dersi müfredatına dayalı olarak yürütülecektir.

Bu çalışmada velisi bulunduğunuz öğrencimizin görüşlerini alabileceğimiz birtakım formları doldurmasını bekleyeceğiz. Bu çalışma sürecine katılım gönüllülük esasına dayalıdır. Bu nedenle isterseniz öğrencimiz çalışmaya katılmayabilir veya doldurmuş olduğu verinin silinmesini talep edebilir, edebilirsiniz. Bu istek hemen yerine getirilecek, siz ve öğrencimiz için herhangi bir olumsuzluk doğurmayacaktır. Bu araştırma için Millî Eğitim Bakanlığı'ndan gerekli izinler alınmıştır. Araştırma için ayrıca "Hacettepe Üniversitesi Etik Komisyonundan" da izin alınmıştır. Çalışmada toplanan veriler sadece çalışmada ismi geçen araştırmacılar tarafından incelenecek ve üçüncü kişilerle asla paylaşılmayacaktır. Çalışma bittikten sonra araştırmacılardan çalışmanın sonuçları hakkında bilgi alabilirsiniz. Bu sonuçlar ve aklınıza gelen herhangi bir başka soru için aşağıda bulunan e-posta aracılığıyla araştırmacılar ile çekinmeden iletişime geçebilirsiniz.

Yukarıda yazılanları okudum ve bahsedilen çalışmaya velisi bulunduğum …….. 'nın tamamen kendi isteğimiz ile katılmasını kabul ediyorum.

Katılımcı:	
Veli Adı Soyadı:	
Tarih:	
İmza:	

Araştırmacı:		**Danışman:**	
Adı ve Soyadı:	Fatma GÖLPEK SARI	***Adı ve Soyadı:***	Prof. Dr. Süleyman Sadi SEFEROĞLU
Adres:	Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü	***Adres:***	Hacettepe Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Tarih:		***Tarih:***	
İmza:		***İmza:***	

EK-Ş. Etik Komisyon Onay Bildirimi

Tarih: 12/11/2019
Sayı: 35853172-300-E.00000857036
0000857036

T.C.
HACETTEPE ÜNİVERSİTESİ
Rektörlük

Sayı : 35853172-300
Konu : Fatma GÖLPEK SARI (Etik Komisyon İzni)

EĞİTİM BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 14.10.2019 tarihli ve 51944218-300/00000814951 sayılı yazı.

Enstitünüz Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Doktora öğrencilerinden **Fatma GÖLPEK SARI**'nın **Prof. Dr. Süleyman Sadi SEFEROĞLU** danışmanlığında yürüttüğü "**Bilgi Güvenliği Farkındalığına Yönelik Bir Çevrimiçi Ortam Tasarımının Öz Düzenleme Stratejileri Açısından Değerlendirilmesi**" başlıklı tez çalışması Üniversitemiz Senatosu Etik Komisyonunun **05 Kasım 2019** tarihinde yapmış olduğu toplantıda incelenmiş olup, etik açıdan uygun bulunmuştur.

Bilgilerinizi ve gereğini saygılarımla rica ederim.

e-imzalıdır
Prof. Dr. Rahime Meral NOHUTCU
Rektör Yardımcısı

Hacettepe Üniversitesi Rektörlük 06100 Sıhhiye-Ankara
Telefon:0 (312) 305 3001-3002 Faks:0 (312) 311 9992 E-posta:yazimd@hacettepe.edu.tr İnternet
Adresi: www.hacettepe.edu.tr
Sevda TOPAL

EK-T. Ankara Valiliği Milli Eğitim Müdürlüğü Araştırma İzni

T.C.
ANKARA VALİLİĞİ
Milli Eğitim Müdürlüğü

Sayı : 14588481-605.99-E.24100798 04.12.2019
Konu : Araştırma İzni

HACETTEPE ÜNİVERSİTESİNE
(Eğitim Bilimleri Enstitüsü Müdürlüğü)

İlgi : a)MEB Yenilik ve Eğitim Teknolojileri Genel Müdürlüğünün 2017/25 nolu Genelgesi.
b)22.11.2019 tarihli ve 300 sayılı yazınız.

Enstitünüz Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı doktora programı öğrencilerinden Fatma GÖLPEK SARI'nın **"Bilgi Güvenliği Farkındalığına Yönelik Bir Çevrimiçi Ortam Tasarımının Öz Düzenleme Stratejileri Açısından Değerlendirilmesi"** konulu çalışması kapsamında İlimize bağlı, ekli listede belirtilen okullarda uygulama talebi ilgi (b) Genelge çerçevesinde incelenmiştir.

Yapılan inceleme sonucunda, söz konusu araştırmanın Müdürlüğümüzde muhafaza edilen ölçme araçlarının; Türkiye Cumhuriyeti Anayasası, Milli Eğitim Temel Kanunu ile Türk Milli Eğitiminin genel amaçlarına uygun olarak, ilgili yasal düzenlemelerde belirtilen ilke, esas ve amaçlara aykırılık teşkil etmeyecek, eğitim-öğretim faaliyetlerini aksatmayacak şekilde okul ve kurum yöneticilerinin sorumluluğunda gönüllülük esasına göre uygulanması Müdürlüğümüzce uygun görülmüştür.

Bilgilerinizi ve gereğini rica ederim.

Turan AKPINAR
Vali a.
Milli Eğitim Müdürü

Dağıtım:
Gereği:
Hacettepe Üniversitesi

Bilgi:
Çankaya, Çubuk, Yenimahalle
İlçe MEM

Adres: Emniyet Mah. Alparslan Türkeş Cad. 4/A
Yenimahalle/ANKARA
e-posta: istatistik06@meb.gov.tr

Bilgi için: D. KARAGÜZEL
Tel: 0 (312) 306 89 07
Faks: 0 (___) ___ __ __

EK-U. Çocuğa Kendini Koruma Bilinci Kazandırma Amaçlı Çevrimiçi Ortamlar Ölçeği Kullanım İzni

Mukaddes Erdem <mukaddese@gmail.com 27 Nis 2021 20:17

Sayın Araştırmacı Fatma Gölpek Sarı,

Seçil Eren ve Mukaddes Erdem tarafından geliştirilen "Çocuğa Kendini Koruma Bilinci Kazandırma Amaçlı Çevrimiçi Ortamlar Ölçeği"ni doktora tezinizde kullanabilirsiniz.

Ölçeğin bağlantı adresi aşağıda yer almaktadır.

https://dergipark.org.tr/en/download/article-file/1160246

İyi çalışmalar,

.....

Prof. Dr. Mukaddes Erdem
Hacettepe Üniversitesi Eğitim Fakültesi
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü

H.Ü. Beytepe Kampüsü D Blok Giriş Kat. Çankaya/Ankara
+90 312 297 71 76
erdemm@hacettepe.edu.tr

EK-Ü. Etik Beyanı

Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı bütün bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin bütününü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

09 / 12 / 2021

Fatma GÖLPEK SARI

EK-V. Doktora Tez Çalışması Orijinallik Raporu

08 / 12 / 2021

HACETTEPE ÜNİVERSİTESİ
Eğitim Bilimleri Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalı Başkanlığına,

Tez Başlığı: Bilgi Güvenliğine Yönelik Çevrimiçi Eğitimin Ortaokul Öğrencilerinin Sanal Ortamlarda Bilgi Güvenliğine İlişkin Öğrenmelerine Etkisi

Yukarıda başlığı verilen tez çalışmamın tamamı (kapak sayfası, özetler, ana bölümler, kaynakça) aşağıdaki filtreler kullanılarak **Turnitin** adlı intihal programı aracılığı ile kontrol edilmiştir. Kontrol sonucunda aşağıdaki veriler elde edilmiştir:

Rapor Tarihi	Sayfa Sayısı	Karakter Sayısı	Savunma Tarihi	Benzerlik Oranı	Gönderim Numarası
08 / 12 / 2021	195	310,928	10 / 11 / 2021	%13	1724620959

Uygulanan filtreler:
1. Kaynaklar hariç
2. Alıntılar dâhil
3. 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Eğitim Bilimleri Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan eder, gereğini saygılarımla arz ederim.

Ad Soyadı: **Fatma GÖLPEK SARI**
Öğrenci No.: N13242027
Ana Bilim Dalı: Bilgisayar ve Öğretim Teknolojileri Eğitimi
Programı: Bilgisayar ve Öğretim Teknolojileri Eğitimi
Statüsü: ☐ Y. Lisans ☒ Doktora ☐ Bütünleşik Dr.

İmza

DANIŞMAN ONAYI

UYGUNDUR
Prof. Dr. Süleyman Sadi SEFEROĞLU

EK-Y. Dissertation Originality Report

08 / 12 / 2021

HACETTEPE UNIVERSITY
Graduate School of Educational Sciences
to the Department of Computer Education and Instructional Technology

Dissertation Title: The Effect of Information Security Online Training on Secondary School Students' Information Security Learning in Online Environments

The whole thesis that includes the *title page, introduction, main chapters, conclusions and bibliography section* is checked by using **Turnitin** plagiarism detection software take into the consideration requested filtering options. According to the originality report obtained data are as below.

Time Submitted	Page Count	Character Count	Date of Dissertation Defense	Similarity Index	Submission ID
08 / 12 / 2021	195	310,928	10 / 11 / 2021	13%	1724620959

Filtering options applied:

1. Bibliography excluded
2. Quotes included
3. Match size up to 5 words excluded

I declare that I have carefully read Hacettepe University Graduate School of Educational Sciences Guidelines for Obtaining and Using Thesis Originality Reports; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

Name Lastname: **Fatma GÖLPEK SARI**

Student No.: N13242027

Department: Computer Education and Instructional Technology

Program: Computer Education and Instructional Technology

Signature

Status: ☐ Masters ☒ Ph.D. ☐ Integrated Ph.D.

ADVISOR APPROVAL

APPROVED
Prof. Dr. Süleyman Sadi SEFEROĞLU

EK-Z. Yayımlama ve Fikrî Mülkiyet Hakları Beyanı

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kâğıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinlerin yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan "**Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına ilişkin Yönerge**" kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü/Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihinden itibaren 2 yıl ertelenmiştir. (1)
- Enstitü/Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren … ay ertelenmiştir. (2)
- Tezimle ilgili gizlilik kararı verilmiştir. (3)

09 / 12 / 2021

Fatma GÖLPEK SARI

"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"

(1) Madde 6. 1. Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma *sürecinin devam etmesi durumunda, tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü Üzerine enstitü veya fakülte yönetim kurulu iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.*

(2) Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç; imkânı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez danışmanın önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulunun gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.

(3) Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, tezin yapıldığı kurum tarafından verilir. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, ilgili kurum ve kuruluşun önerisi ile enstitü veya fakültenin uygun görüşü Üzerine üniversite yönetim kurulu tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.*
Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir

** Tez danışmanının önerisi ve enstitü anabilim dalının uygun görüşü üzerine enstitü veya fakülte yönetim kurulu tarafından karar verilir.*