T.C.
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANABİLİM DALI
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ BİLİM DALI

BİLGİ GÜVENLİĞİ FARKINDALIĞININ GELİŞTİRİLMESİNDE GÖREV TEMELLİ ÇEVRİMİÇİ ÖĞRENME ORTAMININ ETKİLİLİĞİ

YÜKSEK LİSANS TEZİ

BÜLENT ÖKTELİK

Tez Danışmanı
DOÇ. DR. LEVENT ÇETİNKAYA

ÇANAKKALE – 2022

T.C.
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANABİLİM DALI
BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ BİLİM DALI

BİLGİ GÜVENLİĞİ FARKINDALIĞININ GELİŞTİRİLMESİNDE GÖREV TEMELLİ ÇEVRİMİÇİ ÖĞRENME ORTAMININ ETKİLİLİĞİ

YÜKSEK LİSANS TEZİ

BÜLENT ÖKTELİK

Tez Danışmanı
DOÇ. DR. LEVENT ÇETİNKAYA

ÇANAKKALE – 2022

T.C.
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Bülent ÖKTELİK tarafından Doç. Dr. Levent ÇETİNKAYA yönetiminde hazırlanan ve **26/08/2022** tarihinde aşağıdaki jüri karşısında sunulan **"Bilgi güvenliği farkındalığının geliştirilmesinde görev temelli çevrimiçi öğrenme ortamının etkililiği"** başlıklı çalışma, Çanakkale Onsekiz Mart Üniversitesi Lisansüstü Eğitim Enstitüsü **Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı**'nda **YÜKSEK LİSANS TEZİ** olarak oy birliği ile kabul edilmiştir.

Jüri Üyeleri	**İmza**
Doç. Dr. Levent ÇETİNKAYA (Danışman)	……
Prof. Dr. Mustafa Yunus ERYAMAN	……
Doç. Dr. Nihat Gürel KAHVECİ	…….

Tez No : 10353451
Tez Savunma Tarihi : 26/08/2022

Doç. Dr. Yener PAZARCIK
Enstitü Müdürü

../../20..

ETİK BEYAN

Çanakkale Onsekiz Mart Üniversitesi Lisansüstü Eğitim Enstitüsü Tez Yazım Kuralları'na uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi taahhüt ve beyan ederim.

Bülent ÖKTELİK
26/08/2022

TEŞEKKÜR

Araştırmamın her aşamasında değerli vaktini, bilgi ve deneyimlerini esirgemeyen, çalışmam boyunca sabırla ve anlayışla destek olan, cesaretlendirilen, yol gösteren, her zaman öğrencisi olmaktan gurur ve onur duyduğum saygı değer danışman hocam Doç. Dr. Levent ÇETİNKAYA'ya bu güzel süreç için teşekkürü borç bilirim. Tüm süreç boyunca sorulan her soruya sabırla cevap veren ve desteklerini eksik etmeyen Dr. Öğretim Üyesi Can GÜLDÜREN'e, çalışmam boyunca tüm zorlukları benimle birlikte göğüsleyen sevgili Hasan BALCI ve diğer arkadaşlarıma, bu uzun çalışma sürecinde hiç yalnız bırakmayan, beni cesaretlendiren ve hep destek olan sevgilime, desteğini hayat boyu benden esirgemeyen, yürüdüğüm yolda beni hiç yalnız bırakmayan annem Kadriye ÖKTELİK, babam Abidin ÖKTELİK ve sevgili kardeşlerime her şey için sonsuz teşekkürlerimi sunarım.

Bülent ÖKTELİK

Çanakkale, Ağustos 2022

ÖZET

BİLGİ GÜVENLİĞİ FARKINDALIĞININ GELİŞTİRİLMESİNDE GÖREV TEMELLİ ÇEVRİMİÇİ ÖĞRENME ORTAMININ ETKİLİLİĞİ

Bülent ÖKTELİK
Çanakkale Onsekiz Mart Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Yüksek Lisans Tezi
Danışman: Doç. Dr. Levent ÇETİNKAYA
26/08/2022, 102

Bu araştırmada, ilköğretim düzeyi ortaokul kademesinde öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini arttırmaya yönelik görev temelli çevrimiçi öğrenme ortamı geliştirilmesi ve etkililiğinin belirlenmesi amaçlanmıştır. Aynı zamanda bu araştırmanın diğer amacı ise, öğrencilerin geliştirilen öğrenme ortamına ve sürecine yönelik görüşlerinin belirlenmesidir. Bu bağlamda iki aşamadan oluşan çalışmanın ilk aşamasında alanyazında ortaokul düzeyine uygun bir ölçek yer almadığından dolayı ortaokul düzeyinde öğrenim gören öğrencilerin bilgi güvenliği farkındalığını belirlemeye yönelik bir ölçek geliştirilmiştir. İlk aşamada 410 katılımcı grubuyla Açımlayıcı Faktör Analizi (AFA) yapılmış ve ölçeğin üç alt boyut altında (“çevrimiçi güvenlik farkındalığı”, “çevrimiçi merak” ve “siber tehdit farkındalığı”) 30 maddeden oluştuğu belirlenmiştir. AFA’nın ardından elde edilen ölçme aracı 265 kişilik katılımcı grubuna uygulanmış ve gerçekleştirilen Doğrulayıcı Faktör Analizi sonucu 3 faktörlü yapı doğrulanmıştır. Ölçeğin tamamı için Cronbach alfa güvenirlik katsayısı ,90; her alt boyut için Cronbach Alfa katsayısı sırasıyla ,94, ,90 ve ,86 olarak hesaplanmıştır. Çalışmanın ikinci aşaması karma araştırma yönteminden açıklayıcı sıralı desen modelinde tasarlanmıştır. Çalışmanın nicel boyutunda, yarı deneysel yöntemden öntest-sontest kontrol gruplu 2X2’lik split plot desen kullanılmıştır. 20’si deney grubu, 20’si kontrol grubu olmak üzere toplam 40 öğrenci ile gerçekleştirilen çalışmada yapılan analizler sonucunda deney ve kontrol grubu öğrencileri üzerinde gerçekleştirilen öntest bilgi güvenlik farkındalık düzeyi puanları kontrol altına alındığında, deney ve kontrol gruplarının düzetilmiş sontest bilgi güvenliği farkındalık düzeyi puanları gruplama ana etkisinin anlamlı bir farklılık gösterdiği sonucuna ulaşılmıştır.

Çalışmanın açık uçlu soru formuyla toplanan verilerin içerik analizi teknikleriyle analiz edildiği nitel boyutunda ise geliştirilen öğrenme ortamının ilgi çekici olduğu, yönergelerin anlaşılır şekilde sunulduğu ve kullanıcı dostu bir tasarıma sahip olduğu yönünde öğrencilerin görüş bildirdikleri belirlenmiştir. Ayrıca görevler sonrası verilen ödüllerin (rozet ve sertifikalar) öğrencileri olumlu yönde motive ettiği ve öğrencilerin geliştirilen öğrenme ortamını farklı derslerde de kullanmak istedikleri sonucuna ulaşılmıştır. Tüm bu sonuçlar göz önünde bulundurularak görev temelli çevrimiçi öğrenme ortamının öğrencilerinin bilgi güvenliği farkındalık düzeylerini artırmada etkili bir ortam olduğu ve hazırlanan görevlerin etkili görevler olduğu belirlenmiştir. Bu doğrultuda, çalışmanın sonunda uygulama süreci ve araştırmacılara yönelik önerilerde bulunulmuştur.

Anahtar Kelimeler: Bilgi Güvenliği, Bilgi Güvenliği Farkındalığı, Farkındalığın Belirlenmesi, Bilinçlendirme, Görev Temelli Çevrimiçi Öğrenme

ABSTRACT

THE EFFECTIVENESS OF TASK-BASED ONLINE LEARNING ENVIRONMENT IN DEVELOPING INFORMATION SECURITY AWARENESS

Bülent ÖKTELİK

Çanakkale Onsekiz Mart University

School of Graduate Studies

Master of Science Thesis in Computer Education and Instructional Technology

Advisor: Assoc. Prof. Dr. Levent ÇETİNKAYA

26/08/2022, 102

In this research, it is aimed to develop a task-based online learning environment to increase the information security awareness levels of students studying at the middle school level of primary education and to determine its effectiveness. Also, the other aim of this research is to determine the opinions of the students about the developed learning environment and process. In this context, in the first stage of the study, a scale suitable for the middle school level has been developed by the researcher since no scale has been developed in the literature to determine the information security awareness of students studying at the middle school level. In the first stage, Exploratory Factor Analysis (EFA) has been conducted with a group of 410 participants and it has been determined that the scale consists of 30 items under three sub-dimensions ("online security awareness", "online curiosity" and "cyber threat awareness"). The measurement tool obtained after the EFA has been applied to a group of 265 participants and the 3-factor structure has been confirmed as a result of the Confirmatory Factor Analysis. The Cronbach's alpha reliability coefficient for the whole scale has been calculated as ,90; Cronbach's Alpha coefficient for each sub-dimension has been calculated as ,94, ,90 and ,86 respectively. The second stage of the study is designed in the explanatory sequential design model from the mixed research method. In the quantitative aspect of the study, a 2X2 split plot design with pretest-posttest control group from the quasi-experimental method is used. As a result of the analysis of the study conducted with a total of 40 students, 20 in the experimental group and 20 in the control group, it is concluded that when the pretest information security awareness level scores of the experimental and control group students are taken under control, the main effect of

grouping the adjusted posttest information security awareness level scores of the experimental and control groups shows a significant difference. In the qualitative aspect of the study, in which the data collected through an open-ended questionnaire analysed with content analysis techniques, it is concluded that the students have reported that the learning environment developed is interesting, that the instructions are presented in an understandable way and that it has a user-friendly design. It has also been concluded that the rewards given after the tasks (badges and certificates) have motivated the students positively and that the students want to use the developed learning environment in different courses. Considering all these results, it is determined that the task-based online learning environment is an effective environment in increasing students' information security awareness levels and that the tasks prepared are effective. In this regard, at the end of the study, suggestions have been made for the implementation process and researchers.

Keywords: Information Security, Information Security Awareness, Determining Awareness, Raising Awareness, Task-Based Online Learning

İÇİNDEKİLER

Sayfa No

ÜÇÜNCÜ BÖLÜM

ARAŞTIRMA YÖNTEMİ/MATERYAL YÖNTEM

SİMGELER VE KISALTMALAR

AFA	Açımlayıcı Faktör Analizi
BG	Bilgi Güvenliği
BGF	Bilgi Güvenliği Farkındalığı
DFA	Doğrulayıcı Faktör Analizi
GTÖ	Görev Temelli Öğrenme
KMO	Kaiser-Meyer-Olkin Testi
KVKK	Kişisel Verilen Korunumu Kanunu
MEB	Millî Eğitim Bakanlığı
OBGFÖ	Ortaokul Düzeyi Bilgi Güvenliği Farkındalık Ölçeği
TDK	Türk Dil Kurumu
ss	Standart Sapma
df	Serbestlik Derecesi
p	Anlamlılık Düzeyi
t	T testi değeri

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

BİRİNCİ BÖLÜM
GİRİŞ

1.1. Problem Durumu

Geçmişten günümüze topluluklar kazandıkları tecrübeleri bilgiye dönüştürüp nesilden nesile devretmişlerdir (Yenal, 2009). Bu bilgi aktarımı geçmişte ilkel birçok yoldan gerçekleşirken günümüz dünyasında teknolojinin kazandırdıklarından yararlanıp çevrimiçi ortamlarda depolanarak tüm insanlar tarafından erişilebilir hale gelmiştir. Küreselleşmenin gerçekleşmesinde rol oynayan kavramlar arasında "bilgi" ve "teknoloji" kavramları önemli yer tutmaya (Yılmaz ve Horzum, 2005) ve günlük yaşamın vazgeçilmez unsurları haline gelmeye başladığı görülmektedir. Türk Dil Kurumu'na göre teknoloji "İnsanın maddi çevresini denetlemek ve değiştirmek amacıyla geliştirdiği araç gereçlerle bunlara ilişkin bilgilerin tümü" şeklinde tanımlanmaktadır (TDK, 2022). Teknoloji kavramını değişimin hızlı olduğu ve çevrimiçi ortamın insanları sarmaladığı günümüz dünyasında toplumlardan bağımsız düşünmek imkansız hale gelmiştir (Yeşilorman ve Koç, 2014). Teknolojinin de yardımıyla çevrimiçi ortamda bulunan veri parçaları dünyanın tamamına yayılarak bilgiyi küreselleşmiştir. Türk Dil Kurumu'na göre bilgi ise "İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf." olarak tanımlanmaktadır (TDK, 2022). Bilginin iletimi toplulukların daha hızlı gelişebilmesi adına son derece önem taşımaktadır (Webster, 2014). Bu nedenle insanlar bilgiye erişmek, bilgiyi kullanmak ve bilgiye sahip olmak için uğraş göstermektedir (Dura ve Atik, 2002). Bilgiyi ve bilgi kaynağını yaratan bilgi ve teknolojilerin toplumun her alanında yaygın kullanılması nedeniyle toplumsal değişimi harekete geçirdiğine tanık olmaktayız (Bensghir, 1996). Bu anlamda insanların üzerinde büyük bir etkisi olan ve gelişmiş toplumların güçlü araçları olarak karşımıza çıkan bilgi teknolojilerinin günümüzde yaygınlaştığı görülmektedir (Tandoğan vd., 1998). Bilgi toplumu çağında bilginin kaynak olarak kullanılmasıyla üretilen teknolojiler bu çağın birer parçasıdır (Parlar, 2012) ve bu teknolojilerden biri olan internet teknolojisi, "ağların ağı" anlamına gelmekte olup dünyadaki bütün teknolojik cihazların birbiriyle etkileşim içerisinde olmasını sağlayan bir sistem olarak tanımlanmaktadır (Geray, 2002). Özellikle mobilleşme ile birlikte hızla yaygınlaşan internet teknolojilerine karşı insanların ilgileri her geçen gün artmış ve yaşamlarının merkezine oturan yapılar haline gelmiştir. Bireyler arası etkileşim ve

beraberinde toplumsal yapı üzerinde hızla etkisini göstermeye başlaması bu teknolojilerin günlük yaşamın bir parçası haline gelmiş ve bireylerin bu yeni yaşam tarzına ayak uydurmalarını da zorunlu kılmıştır (Cetinkaya, 2017). Her ne kadar yaşamı kolaylaştırdığından dolayı bu teknolojilerin kabulü büyük oranda kolay olmuş olsa da bu teknolojilerin kullanımına karşı direnenler de kullanmak zorunda kalmışlardır. Geldiğimiz son noktada kullanımının gerekliliği bir tartışma konusu olmaktan çıkarak günlük yaşamın bir parçası haline gelen bu teknolojilerin doğru bir şekilde kullanımına odaklanılmaya başlanmıştır.

Günümüzde internet banka işlemleri, alışveriş, oyun oynamak, fatura ödemeleri, iletişim kurmak, araştırma yapmak, fotoğraf veya video çekmek ve birçok şey için aktif olarak kullanılmaktadır (Mestçi, 2007). İnternet sayesinde insanlar dünyanın herhangi bir yerinden biriyle kolaylıkla iletişim kurmakta, onların kültürleri ve yaşam şartları hakkında bilgi edinebilmektedir (Güçdemir, 2003). Diğer taraftan internet teknolojisinin bu denli gelişiminden dolayı bilgi üretimi son dönemde büyük önem kazanırken ülkeler arasında rekabet öğesi haline gelmiş ve bu durum bilgi güvenliği kavramıyla ile ilgili problemlerin de ortaya çıkmasına sebep olmuştur. Bilgi teknolojilerinin bir alt kümesi olarak kabul edilen bilgi güvenliği (Haufe vd., 2016), bireylere ya da kurumlara ait olan bilgilerin üçüncü kişilerin eline geçmemesi adına alınan önlemler olarak tanımlanmaktadır (Canbek ve Sarıoğlu, 2006). Günümüz dünyasında dijitalleşme sürecininin başarısını doğrudan etkileyecek kadar kritik bir unsur olan bilgi güvenliği; bilgiyi kullanan, saklayan ve aktaran sistemleri ile birlikte bilginin korunması, veri güvenliği ve ağ güvenliği gibi önemli bileşenleri bir arada bulundurmaktadır (Koohang vd., 2020). Son yıllarda bilgi güvenliğine duyulan ihtiyaç beraberinde bilgi güvenliği farkındalığı kavramını da ortaya çıkarmıştır. Bilgi güvenliği farkındalığı, bilgi güvenliğini etkilemekle birlikte eksikliği söz konusu olduğunda güvenlik açıklarının ve güvenlik tehditlerinin arttığı görülmektedir (AlKalbani vd., 2015; Chandarman ve Van Niekerk 2017; Hanus ve Wu, 2016; Öztezcan ve Çetinkaya, 2017). Alanyazında bilgi güvenliği ihlallerinin genellikle; doğrudan, kazara veya kötü niyetli insan faktörlü hatalara bağlı olduğu vurgulanmaktadır (Pricewaterhouse Coopers, 2015). Bundan dolayı bilgi güvenliği tehditlerini tamamen bitirmek mümkün olmasa da farkındalık eğitimi ile güvenlik tehditlerinin en aza indirilmesi mümkün olabilir (Acılar, 2009; Güldüren vd., 2016; Gülmüş, 2010). Bu anlamda bilgi güvenliği farkındalık

eğitimlerini ve güvenlik stratejilerini kullanabilmek bilgi güvenliği risklerinden korunmak adına önem arz etmektedir (Puhakainen, 2006, Siponen, 2001).

Bireylerin her geçen gün artan çevrimiçi teknolojilere bağlı kalma isteği, bireylerin çevrimiçi risklere daha fazla maruz kalmasına sebep olmaktadır (Mochiko, 2016). Her ne kadar çevrimiçi teknolojiler iletişim ve sosyalleşme konusunda büyük yararlar sunsa da çocukları çeşitli risklerle karşı karşıya bırakabilmektedir (Çelen vd., 2011). Söz konusu bu riskler, kötü amaçlı yazılımlar (virüs, trojen vb.), casus yazılımlar, bilgisayar korsanlığı, sosyal mühendislik ve siber zorbalık gibi çok çeşitli olabilmektedir (Çakır ve Kesler, 2012; Keser ve Güldüren, 2015; Lee, 2021). Bu riskler her yaş grubundan bireyleri tehdit etse de gelişim çağındaki çocukların güncel teknolojileri kullanma istekleri ve karşılaşabilecekleri riskler hakkında bilgi eksiklikleri gibi sebepler nedeniyle daha kolay birer hedef haline geldiği görülmektedir (Atkinson vd., 2009; Güldüren vd., 2016; Pattinson vd., 2015). Bunun yanı sıra okullardaki hızlı dijitalleşme süreci ile birlikte teknoloji odaklı yenilikçi öğrenme yöntemlerinin hayata geçmeye başladığı görülmektedir. Bu durum kişisel kullanımın yanı sıra eğitsel amaçlı da çevrimiçi ortamların kullanım sıklığını artırarak çocukların bilgi güvenliği tehditleriyle daha çok karşılaşma olasılıklarını arttıracaktır. Bu bağlamda bilgi güvenliği farkındalığını sağlamak için öncelikle eğitim programları oluşturulması ve çocuklara bilgi güvenliği kavramının, karşılaşabilecekleri risklerin uğratacağı hasarı en aza indirebileceği eğitim programları aracılığıyla aktarılması gerekmektedir (Brady, 2010; Güldüren vd., 2016; Whitman ve Mattord, 2018).

Bilgi güvenliği farkındalığının kazandırılmasına yönelik eğitim faaliyetleri için özellikle ortaöğretim düzeyinin en uygun dönem olduğu ifade edilmektedir (Bintziou vd., 1999). Bu çağda bireyler bilgisayar, akıllı telefon, tablet gibi teknolojilerle ilk defa ciddi anlamda karşılaşmakta ve korunmaya ihtiyaç duymaktadır. Bundan dolayı çocukların bilgi güvenliği farkındalığı kazanması bakımından eğitim faaliyetlerine doğrudan dahil olması gerekmektedir (Atkinson vd., 2009). Bunun sonucunda bilgi güvenliği farkındalığı kazanan çocuklar kendi güvenliklerini sağlama konusunda çaba sarf edecekler ve olası risklerin en aza indirgenmesini sağlayabileceklerdir. Günümüzde büyük bir hızla teknolojinin eğitim ortamlarına entegre olmaya başladığı görülmektedir. Bundan dolayı eğitim kurumlarında bilgi güvenliği farkındalığının sağlanması bir ihtiyaç haline gelmiştir. Bu süreçte ise bilgi

güvenliği farkındalığının kazandırılmasına ve arttırılmasına yönelik geliştirilen eğitim programlarında bireylerin bilgi düzeyleri ve beklentileri göz önünde bulundurulması gerekmektedir (Şahinaslan vd., 2009). Bu anlamda farkındalığın belirlenmesi ve bu çerçevede bilgi güvenliği yeterliliklerin kazandırılması noktasında önlemlerin alınması önemlidir. Özellikle bilgi güvenliğinin sağlanmasında "zayıf halka" olarak tanımlanan insan faktörünün göz ardı edilmemesi (Kritzinger ve Smith, 2008; Veiga, 2008) ve bu anlamda erken dönemde durum tespiti ile birlikte önleyici tedbirlerin alınması gerekmektedir. Bilgi güvenliğine yönelik yapılan araştırmalar göz önünde bulundurulduğunda genellikle insan faktörünün göz ardı edildiği ve daha çok bilginin korunmasına yönelik teknolojik sorunların çözümüne odaklanıldığı görülmektedir (Esteves vd., 2017; Gao vd., 2022; Öztemiz ve Yılmaz, 2013). Oysaki dijitalleşme sürecinde bilginin depolanmasından yönetimine kadar tüm süreçlerinde insan vardır ve insana yönelik faktörler dikkatle ele alınmalıdır (Ki-aries ve Faily, 2017). Özellikle internet temelli teknolojiler ile beraberindeki uygulamaların yaygınlaşmasının da etkisiyle son dönemlerde bilgi güvenliğinde insan faktörünü ön plana alan ve özellikle çocukların bilgi güvenliğine yönelik öz değerlendirme yapabilmelerinin önemine vurgu yapan çalışmalar hız kazanmaya başlamıştır. Yine bu çalışmalarda başta çevrimiçi ortamlar olmak üzere olası tehlikelerden korunabilmenin önemi ile birlikte bu konuda eğitimler ve bilinçlendirme çalışmaları yapılması gerekliliği net bir şekilde vurgulanmaktadır (Allers vd., 2021; Güldüren vd., 2016; Karaahmetoğlu, 2021; Mahabi, 2010; Theofanos vd., 2021). Bilgi güvenliği farkındalığı kazandırılmasına yönelik verilecek eğitimlerde ise öğrencilerin bizzat sürece aktif olarak dahil olmaları konusunda araştırmacıların çoğunluğunun hemfikir olduğu görülmektedir (Atkinson vd., 2009; Güldüren vd., 2016). Nitekim bu eğitimler bireylerin bilgi güvenliği farkındalığını sağlanmasının yanı sıra internet ya da teknoloji temelli risklerden de kaçınmalarına katkı sağlayacaktır. Bu noktada risklerin okul içerisinde öğrenciler arasında kolay bir şekilde yayılabilecek eylemler haline gelebileceği düşünülerek önüne geçmek adına kayıtsız kalınmaması gerekmektedir. Aksi takdirde bilgi güvenliği kaynaklı riskler geleceğin en önemli sorunları olarak karşımıza çıkacak ve zamanla büyüyen problemlerin ortaya çıkmasına neden olacaktır. Yine bu durum günümüz gençlerinin kişisel ve akademik gelişimlerini olumsuz yönde etkileyerek telafisi güç sonuçların ortaya çıkmasına yol açacaktır. Bu noktada bilgi güvenliğine yönelik risklere karşı erken dönemde işlevsel, gerçekçi, dinamik ve süreklilik arz eden farkındalık eğitimlerinin yanı sıra aktif öğrenme

sürecini destekleyebilecek nitelikte kişiselleştirilebilir eğitim materyallerinin geliştirilmesi gerekmektedir.

1.2. Araştırmanın Amacı

Bu araştırmada, ilköğretim düzeyi ortaokul kademesinde öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini arttırmaya yönelik görev temelli çevrimiçi öğrenme ortamı geliştirilmesi ve etkililiğinin belirlenmesi amaçlanmıştır. Aynı zamanda bu araştırmanın diğer amacı ise, öğrencilerin geliştirilen öğrenme ortamına ve sürecine yönelik görüşlerinin belirlenmesidir. Bu amaçlar doğrultusunda aşağıdaki sorulara yanıt aranmaktadır;

1. Deney ve kontrol grubu öğrencilerinin öntest bilgi güvenliği farkındalık düzey puanları arasında anlamlı bir farklılık var mıdır?
2. Deney ve kontrol grubu öğrencilerinin öntest-sontest bilgi güvenliği farkındalık düzeyi puanları arasında anlamlı bir farklılık var mıdır?
3. Deney ve kontrol grubu öğrencilerinin bilgi güvenliği farkındalık ölçeği öntest puanları kontrol edildiğinde, sontest bilgi güvenliği farkındalık düzeyi puanları arasında anlamlı bir farklılık var mıdır?
4. Deney grubu öğrencilerinin geliştirilen öğrenme ortamına ve sürecine yönelik görüşleri nelerdir?

1.3. Araştırmanın Önemi

Bilgi ve iletişim teknolojileri, bireylerin geçmişten günümüze geçen süreçte hızla artan bilgiye erişim, bilgiyi paylaşma ihtiyacına yanıt verebilmesi adına hayatın vazgeçilmez bir parçası olmuştur. Özellikle de internet teknolojileri sayesinde mesafe başta olmak üzere etkileşime dair birçok sınır ortadan kalkmaya başlamıştır. Ancak kontrolsüz internet temelli teknolojilerin kullanımı ile bilgi güvenliğine yönelik riskler hızla artarak bireylerin istenmeyen ve telafisi güç sonuçlar ile karşı karşıya kalabilmelerine neden olmaya

başlamıştır. Bu durum başta kişisel veriler olmak üzere kontrolsüzce yayılabilen bilginin güvenliğini sağlanabilmesinin ve farkındalığın kazandırılmasının önemini her geçen gün arttırmaktadır. Bilginin değerli olması bilgiyi ele geçirmeye yönelik tehditlerin ve kullanılan araçların çeşitliliği, bilgi güvenliğini sağlamak amacıyla önlem almanın zorunluluğunu göstermektedir (Horne vd., 2016). Bu önlemler arasında en etkili olanı ise eğitim yoluyla bireyler üzerinde farkındalık yaratmak, bireyleri bilinçlendirmek ve bireylerin bilgiye ulaşma yollarını güvenilir hale getirmektir (Atkinkon vd., 2009, Güldüren vd., 2016). Özellikle ülkemizde, birçok bilgisayar kullanıcısının bilgi ve bilgi güvenliğine bakış açısının yeterli seviyede olmadığı görülmektedir (Kesmez, 2002). Bilgi güvenliği farkındalığı kazandırılmasında kullanılacak olan eğitim materyalinin, farkındalık yaratma, ortak anlayış geliştirme, hedef odaklı çalışma boyutlarından oluşması önerilmektedir (Şahinaslan vd., 2009). Bu bağlamda gerek eğitim materyallerinin geliştirilmesi gerekse eğitimin uygulama sürecinde kullanılabilecek etkili öğretim yöntemlerden birisi de görev temelli çevrimiçi öğrenme yöntemidir. Görev temelli çevrimiçi öğrenmede öğrenciler, görevle ilişkili davranışların altında yatan sebepleri ve ilkeleri temel seviyeden ele almaktadır (Akyüz, 2012). Görev temelli çevrimiçi öğrenmenin en önemli avantajı ise, öğrencinin kendi yeteneklerini kullanma şansı vermesi ve öğrencinin hedef odaklı çalışmasına olanak sağlamasıdır (Pools-m, 2013). Görev temelli öğrenme sırasında oluşan tartışma ortamında öğrenciler, okul yönetimi ve aileleri bir araya getirdiği için bilgi güvenliği farkındalığı kazandırmaya olanak sağlayacaktır. Bu bağlamda bu araştırmada ilköğretim düzeyi ortaokul kademesinde öğrenim gören öğrencilerin bilgi güvenliği farkındalıklarının arttırılmasına yönelik görev temelli çevrimiçi öğrenme ortamının geliştirilmesi ve etkililiğinin belirlenmesi amaçlanmıştır. Aynı zamanda bu araştırma sonunda alanyazında hedef kitle özelliklerine göre geliştirilmiş ölçek bulunmadığından dolayı araştırmacı tarafından ilköğretim düzeyi ortaokul kademesinde kullanılmak üzere geçerli ve güvenilir bir bilgi güvenliği farkındalık ölçeği geliştirilmiştir.

Son yıllarda hızla gelişmekte olan teknolojik değişimlerin başında tüm dünyaya damgasını vuran internet teknolojisi gelmektedir. İnternet teknolojisinin gelmesiyle birlikte bilgiye ulaşma, bilgiyi saklama ve bilgiyi paylaşma kavramları fiziksel olmaktan çıkıp çevrimiçi ortamlardan sağlanabilir hale gelmiştir (Çakır, 2006). İnternetin mobilize olmasından sonra kullanımı daha çok artmış ve bununla beraber bilgi güvenliği kavramı

hayati önem kazanmıştır. Bilginin değerli olmasından kaynaklı bilgiyi ele geçirmeye yönelik oluşan tehditlerin ve kullanılan araçların fazlalığı ile bilgi güvenliği farkındalığının kazandırılması konusu doğru orantıda ilerlemektedir. Bu sebeple dijital vatandaş olma ve dijital vatandaş olma yeterliliğin sağlanması amacıyla özellikle gençlerin bilgi güvenliği farkındalıklarının kazandırılması çok önemlidir. Bu araştırmanın geliştirilen öğrenme ortamıyla ortaokul kademesinde öğrenim gören öğrencilerin bilgi güvenliği tehditlerine karşı risklerin azaltılması için öğrencilere rehberlik edeceği, uygun eğitim materyalleri ve stratejilerin geliştirilmesine katkı sağlayacağı ve kurumlarda bulunan eksikliğin giderilmesi için hazırlanacak eylem planlarına kaynaklık edeceği düşünülmektedir. Bunlara ek olarak, alanyazında ortaokul düzeyi öğrencilerinin bilgi güvenliği farkındalık düzeylerinin belirlenmesi adına görev temelli çevrimiçi öğrenme ortamının etkisi daha önce araştırma konusu yapılmamış olması nedeniyle özgün bir araştırmadır. Araştırma sonunda elde edilecek bulgular doğrultusunda tasarlanacak görev temelli çevrimiçi öğrenme ortamlarıyla etkili, ilgi çekici ve verimli bilgi güvenliği farkındalık eğitimleri yapılabilecektir. Araştırmalarda elde edilen sonuçların bundan sonra yapılacak olan çalışmalara ışık tutacağı düşünülmektedir.

1.4. Varsayımlar

Araştırmaya katılan öğrencilerin geliştirilen ölçme aracına samimi ve doğru cevaplar verdikleri varsayılmıştır.

1.5. Sınırlılıklar

1. Bu araştırmada yer alana bilgi güvenliği kavramı dijital teknoloji temelli bilgi güvenliği konusuyla,
2. Ortaokul kademesinde öğrenim gören 6. sınıf öğrencileriyle,
3. Bilgi güvenliği farkındalığı oluşturmaya yönelik araştırmacı tarafından geliştiriler eğitim materyalleri ile sınırlıdır.

1.6. Tanımlar

Bilgi: Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, vukuf (TDK, 2022).

Güvenlik: Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet (TDK, 2022).

Bilgi Güvenliği: Bilginin bir varlık olarak karşılaşabileceği tüm tehditlere karşı korunması, üçüncü kişilerin eline geçmesinin önlenmesi ve amacı dışı kullanılmasının engellenmesidir (Canbek ve Sarıoğlu, 2006). Bilgi güvenliği, bilgiye yönelik tehditlere ve güvenlik açıklarına karşı korunması olarak da tanımlanabilir.

Bilgi Güvenliği Farkındalığı: Bilgi güvenliği farkındalığı, bilgi güvenliği tehditlerini ve bu tehditlerin önüne geçilmesi hakkında bilgi sahibi olmasıdır (Banerjee, Banerjee ve Murarka 2013). Yine bilgi güvenliği farkındalığı, insanların bilgi güvenliği politikalarının, kurallarının ve yönergelerinin önemi ne ölçüde anladığını ve bilgi güvenliği risklerine karşı ne ölçüde önlem aldığı anlamına gelmektedir (Haeussinger ve Kranz, 2017; Imgraben vd., 2014).

Bilişim: İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimidir (TDK, 2022).

Bilişim Teknolojileri: Bilişimde kullanılan bütün araç ve gereçlerin oluşturduğu sistemdir (TDK, 2022).

Görev Temelli Öğrenme (Task Based Learning): Öğrenmenin sağlanması amacıyla gerekli verilerin öğrenenlere sunulması ve öğrencilerin sahip olduğu bilgi ile görevleri yerine getirmesine dayanan öğrenme-öğretme yöntemi (Harden vd., 1996).

Farkındalık Kazandırma: İnsanları herhangi bir konuda bilinçlendirmek, konuya dikkat çekerek kişilerin o konu hakkında bilgi sahibi olmasını sağlamak (TDK, 2022).

İKİNCİ BÖLÜM
KURAMSAL ÇERÇEVE/ ÖNCEKİ ÇALIŞMALAR

Bu bölümde araştırmaya konu olan temel kavramlara (bilgi güvenliği, bilgi güvenliği farkındalığı, görev temelli çevrimiçi öğrenme) ve ilgili araştırmalara yer verilmiştir.

2.1. Bilgi Güvenliği

Günümüzde bilişim teknolojilerinin aktif kullanılmasıyla bilgiyi üretmek, saklamak, paylaşmak ve kullanmak kolaylaşmıştır (Canbek ve Sağıroğlu, 2006). Bilişim teknolojilerinin aktif olarak kullanılmaya başlanmasıyla beraber bilgi hızla üretilen, geliştirilen ve dağıtılan bir ürün olarak karşımıza çıkmaktadır (Blackley vd., 2004). İnsanlar için en değerli öğe bilgidir ve insanlar bilgiyi, tarih boyunca farklı şekillerde bilgileri depolamış ve saklamıştır. Bu noktada toplumlar için bilgi; üretim, hizmet veya tüketim sürecinde çok değerli ve toplumlar arası değişmez bir rekabet unsuru haline gelmiştir (Eminağaoğlu ve Gökşen, 2009). Bu bağlamda toplum için değişmez bir unsur olan bilginin güvenliğine yönelik bilgi güvenliği kavramı ortaya çıkmıştır. Bilgi güvenliği genel olarak bilginin bir varlık olarak karşılaşabileceği tüm tehditlere karşı korunması, üçüncü kişilerin eline geçmesinin önlenmesi ve amacı dışı kullanılmasının engellenmesi şeklinde tanımlanmaktadır (Canbek ve Sarıoğlu, 2006). Bir başka tanımlama da bilgi güvenliği, bilgiye yönelik tehditlere ve güvenlik açıklarına karşı korunması olarak ifade edilmiştir (von Solms ve van Niekerk, 2013). Horne vd., (2016) ise bilgi güvenliğini, insanların bilinçli veya bilinçsiz olarak bilgiden kaynak yaratma ve tehditlerle karşılaşmamak için kontrol davranışları olduğunu ileri sürmüşlerdir. Bilgi güvenliği kavramı genel olarak gizlilik, bütünlük ve ulaşılabilirlik olmak üzere üç başlık altında toplanmaktadır (Puhakainen, 2006). Bu bileşenlerden birinin zarar görmesi veya ortadan kaybolması durumunda bilgi güvenliği tehlikeye girebilmekte (Daalen, 2022) ve bu tehlikeler ise telafisi güç sonuçlara neden olabilmektedir. Bu üç temel bileşenden biri olan gizlilik, bireylere ya da kurumlara ait kritik verilere ait bilgilere (müşteri bilgileri, kişisel bilgiler, çalışan bilgileri, vb.) yetkisiz kişilerin erişmemesi gerektiğini ifade eder (Koohang vd., 2020; Topa ve Karyda, 2019). Bütünlük ise bilginin değiştirilmemiş ve bozulmamış olması gerektiğini ifade eder (Leszczyna, 2018). Bilgi güvenliğinin diğer bileşeni olan ulaşılabilirlik ise, bireylerin ya da kurumların bilgiye

talebi üzerine günün herhangi bir zaman diliminde erişilebilir olması gerektiğini ifade etmektedir (Whitman ve Mattord, 2018). Bu temel güvenlik unsurlarından herhangi birinin zarar görmesi durumunda güvenlik zafiyetlerinin ortaya çıkması kaçınılmazdır (Daalen, 2022). Bu güvenlik zafiyetlerinin tamamının yok edilmesi her ne kadar mümkün olamasa da olası riskler göz önünde bulundurularak bu risklere yönelik gerekli tedbirlerin alınması noktasında bilgi güvenliğine yönelik farkındalığın oluşturulması önemli bir unsur olarak karşımıza çıkmaktadır.

2.1.1. Bilgi Güvenliği Farkındalığı

Çevrimiçi ortamda, bilgi teknolojileri varlıklarının güvenliğinin sağlanması kurumların kötü niyetli saldırılardan korunması adına en önemli öncelik haline gelmiştir (Sharma ve Aparicio, 2022). Araştırmalarda hem siber suçluların hem de veri ihlallerinin son yıllarda önemli ölçüde arttığı görülmekte (Khando vd., 2021) ve bu nedenle de kurumlar sürekli olarak bilgi teknolojileri varlıklarının güvenliğini sağlamak için mücadele etmekte ve teknolojik temelli tedbirlere büyük yatırımlar yapmaktadır (Spears ve Barki, 2010). Ancak çok disiplinli olması ve insan boyutunun önemli bir rol oynaması gibi nedenlerle doğası gereği bilgi güvenliğinin sadece teknik yönlerine odaklanmak yeterli değildir (Stahl vd., 2012). Nitekim araştırmalar kurumların veri ihlallerinin yaklaşık olarak %77'sinin insan kaynaklı faktörlerden meydana geldiği ve bilgi güvenliği ihlallerinin yarısından fazlasının çalışanların zayıf bilgi güvenliği farkındalıklarından kaynaklandığını göstermektedir (ENISA, 2019; Humaidi ve Balakrishnan, 2015). İnsanların bilgi güvenliği farkındalık düzeyi, bilgi güvenliği davranışları ve kurumların bilgi güvenliği önlem politikası adına önemli bir etkiye sahiptir (DeGroot vd., 2012). Son dönemlerde bilgi güvenliği sağlama konusunda insan unsurunun en zayıf halka olmasından dolayı bilgi güvenliği farkındalığı hem araştırmalarda hem de uygulamada en önemli unsur haline gelmiştir (Haeussinger ve Kranz, 2017; Imgraben vd., 2014). Bu noktada bilgi güvenliği farkındalığı kavramı keşfedilmeyi bekleyen ve birçok keşfedilmemiş kavramlarla birlikte hala gelişmekte olan bir kavram olarak karşımıza çıkmaktadır (Jaeger, 2018).

Bilgi güvenliği farkındalığını ve bu farkındalığa katkıda bulunan faktörleri anlamak bilgi güvenliği risklerini azaltmak adına önem arz etmektedir. Bilgi güvenliği farkındalığı, insanların bilgi güvenliği politikalarının, kurallarının ve yönergelerinin önemini ne ölçüde anladığını ve bilgi güvenliği risklerine karşı ne ölçüde önlem aldığı anlamına gelmektedir (Kruger ve Kearney, 2006; Wiley, McCormac ve Calic, 2020). Parsons vd., (2014) bireylerin bilgi güvenliği farkındalıkları arttıkça bilgi güvenliğine yönelik davranışlarının iyileştiğini belirtmiştir. Ancak bilgi güvenliği farkındalığı eğitim materyallerinin içeriğini geliştirirken insanların bilgi güvenliği farkındalığı düzeylerini etkileyen faktörler göz önünde bulundurulmadığından kurumların bilgi güvenliği eğitimlerinde başarısız oldukları görülmekte ve eğitimlerin geliştirilmesi sırasında ilgi çekici ve işlevsel materyaller oluşturmak için yöntemlerin eksik olduğu görülmektedir (Bada vd., 2019). Bu noktada farkındalık eğitimlerinin işlevsel olması, gerçekçi, dinamik, ilgi çekici ve sürekli olmasının sağlanmasının yanı sıra (Bada vd., 2019) aktif öğrenme sürecini destekleyebilecek nitelikte kişiselleştirilebilir eğitim materyallerinin geliştirilmesi de gerekmektedir.

2.1.2. Bilgi Güvenliğine Yönelik Tehditler

Tehdit; güvenliği ihlal etmek, bilgi güvenliği öğelerini olumsuz yönde değiştirmek, silmek veya zarar vermek için bir güvenlik açığından yararlanarak yapılan her şey olabilir (Can ve Akbaş, 2014). Bilgi güvenliği tehditleri ele alındığında ise;

- Fiziki unsurlardan kaynaklanan tehditler,
- Teknolojik temelli tehditler,
- Organizasyonel tehditler ve
- İnsan unsurundan kaynaklanan tehditler olarak belirtilmektedir (Cherdantseva ve Hilton, 2013; Şahinaslan vd., 2009; Vural, 2007).

Fiziki Unsurlardan Kaynaklanan Tehditler

Fiziki unsurlardan kaynaklanan tehditlerin genel olarak doğal afetlerden dolayı ortaya çıktığı görülmektedir. Doğal afet; genellikle insanların önüne geçemediği ve önlemlerin alınmadığı takdirde birçok kayba yol açan doğa olaylarıdır. Deprem, sel, heyelan,

çığ, yangın gibi doğa olayları doğal afetlere örnek olarak gösterilmektedir. Doğal afetler her ne kadar insan kontrolü dışında gerçekleşse de gerekli önlemler alınarak can ve mal kaybı en aza indirilebilir (Vural, 2007). Doğal afetler beklenmedik anda gerçekleştiğinden dolayı gerekli önlemleri almayan kurumların bilgi güvenliği sistemlerini olumsuz etkilemektedir. Doğal afet olayları dışında fiziki unsurlardan kaynaklanan tehditler;

- Güç kaynağının arızalanması,
- Ağ sisteminin arızalanması,
- Sunucu-istemci sisteminin bozulması,
- Güvenlik sisteminden (kameralar, alarm sistemi vb.) kaynaklı tehditler ve
- Yedekleme sisteminden kaynaklanan tehditler

olarak sıralanabilir (Güldüren, 2015).

Teknolojik Temelli Tehditler

Çevrimiçi saldırganların, bilgi sistemlerinde bulunan açıkları kendi veya üçüncü şahısların çıkarları için kullanarak bilgiye izinsiz erişmelerini sağlayan tehditlerdir ve bilgi güvenliği saldırıların büyük bir çoğunluğunu oluşturmaktadır. En sık karşılaşılan teknolojik temelli saldırılara örnek olarak gösterilebilecek saldırı türleri aşağıda belirtilmiştir.

Kimlik Avı Saldırıları: Kimlik avı saldırıları internet kullanıcılarının finansal ve kişisel bilgilerinin çalınması olarak tanımlanmaktadır (Gupta vd., 2018). Bu saldırı türü internet kullanıcılarının genellikle kişisel verilerine yönelik olmakla birlikte (Jain ve Gupta, 2022) internet kullanıcılarını büyük bir çoğunluğunu etkileyen siber saldırı türüdür. (Almomani vd., 2013). Bu saldırılar genellikle e-posta, sosyal ağlar ve diğer çevrimiçi ortamlar aracılığıyla kullanıcıların kimlik, şifre ve diğer kişisel bilgilerini çalmaya yönelik saldırıları temsil etmektedir (Abdillah vd., 2022). Kimlik avı saldırıları internet kullanıcılarının kişisel bilgilerini tehdit etmekte ve bu saldırılara uğrayan bireylerin kişisel bilgilerini açığa çıkarmaktadır.

İstenmeyen E-Posta Sağanakları (Spam): Yüz milyonlarca kullanıcı, haberleri yaymak, günlük yaşam gibi çeşitli konularda görüşlerini paylaşmak için sık sık e-posta göndermektedir (Internetlivestats, 2022). Bununla birlikte saldırganlar; reklamcılık yapmak, kullanıcıların kişisel bilgilerini toplamak ve web sitelerini tanıtmak vb. olmak üzere çeşitli istenmeyen e-posta sağanakları yayınlamaktadır (Hekim ve Başıbüyük, 2013). Bundan dolayı istenmeyen e-posta sağanakları dolandırıcılık, kötü amaçlı yazılım ve kimlik avı ile ilgili tehlikeli içerikler içerebilmektedir (Hu vd., 2013). Aynı zamanda istenmeyen zararlı e-posta içerikleri kullanıcı deneyimini ciddi şekilde zedelediği ve çevrimiçi kaynakların sağlıklı gelişimini engelleyebileceği düşünülmektedir (Lee vd., 2010).

Casus Yazılımlar (Spyware): Kullanıcıların bilgisayarlarındaki aktivitelerini izleyen ve toplanan kişisel bilgileri üçüncü kişilere aktaran yazılımlar olarak tanımlanan casus yazılımlar genellikle truva atı, virüs ve solucan gibi farklı isimlerle tanımlanan kod parçacıkları aracılığı ile bilgisayarlara aktarılır (Kaspersky, 2022). Genellikle kullanıcıdan habersiz ve kullanıcının izni olmadan arka planda sessizce çalışarak kullanıcıların kişisel bilgilerini toplamak üzerine kurgulanan bu yazılımların en yaygın örneklerinden biri keylogger'dır. Temel işlevi kullanıcıların klavye tuş vuruşlarını kaydetmek olan keylogger çeşitli yazılımlar aracılığıyla kullanıcıların kişisel bilgilerini (kullanıcı adı, şifre, kredi kartı bilgileri vb.) ortaya çıkarmakta (Geeksforgeeks, 2021) ve çoğu zaman telafisi güç olumsuz sonuçlara neden olmaktadır.

Bilgisayar Virüsleri: TDK' ye göre bilgisayar virüsleri, "veri girişi yoluyla bilgisayarlara yüklenen, sistemin veya programların bozulmasına, veri kaybına ve olağan dışı çalışmasına neden olan yazılım" olarak tanımlanmaktadır (TDK, 2022). Alanyazında ise bilgisayar virüsleri, genellikle kullanıcının izni ve yetkisi olmadan bilgisayarlara giren, olağan çalışmayı bozan ve verilere zarar veren bir tür kötü amaçlı yazılım olarak tanımlanmaktadır (Yılmaz ve Salcan, 2008). Bilgisayar virüsleri işleyiş açısından biyolojik virüslere benzer öncelikle virüs vücuda (bilgisayar sistemi) girer, vücuda zarar verir, diğer vücutlara (farklı bilgisayarlara) yayılır ve bağışıklık sistemi veya harici yollarla (anti virüs vb.) yok edilir (Subramanya ve Lakshminarasimhan, 2001). Bundan dolayı bilgisayar virüsleri sistemleri bozma, büyük organizasyonel sorunlara ve veri kaybına neden olmakta olup en önemli özelliği programlar ve sistemler arasında yayılmak üzere tasarlanmış

yapılardır (Fortinet, 2022). Bilgisayar virüslerine karşı geliştirilen anti virüs yazılımları, bilgisayar sistemine virüslerin girişinin engellenmesi, olası risklere karşı sistemin korunması ve var olan güvenlik sorunlarının düzeltilmesi gibi çözümler getirmektedir.

Organizasyonel Tehditler

Organizasyon kavramı, yapılacak işi belirlemek ve gruplandırmak, sorumluluk ve yetkiyi tanımlamak ve beraberinde hedeflere ulaşmada insanların birlikte en etkin şekilde çalışmasını sağlamak amacıyla ilişkiler kurma sürecidir. Organizasyonel tehditler, kurumların organizasyonel süreçleri tamamlayamamasından kaynaklandığı düşünülmektedir (Vural, 2007). İdari ve teknik anlamda gerekli kurallara uyulmadığı takdirde kurumlar bilgi güvenliği tehditlerine açık hale gelebilmektedir (Güldüren, 2015; Vural, 2007).

İdari Eksiklikler:

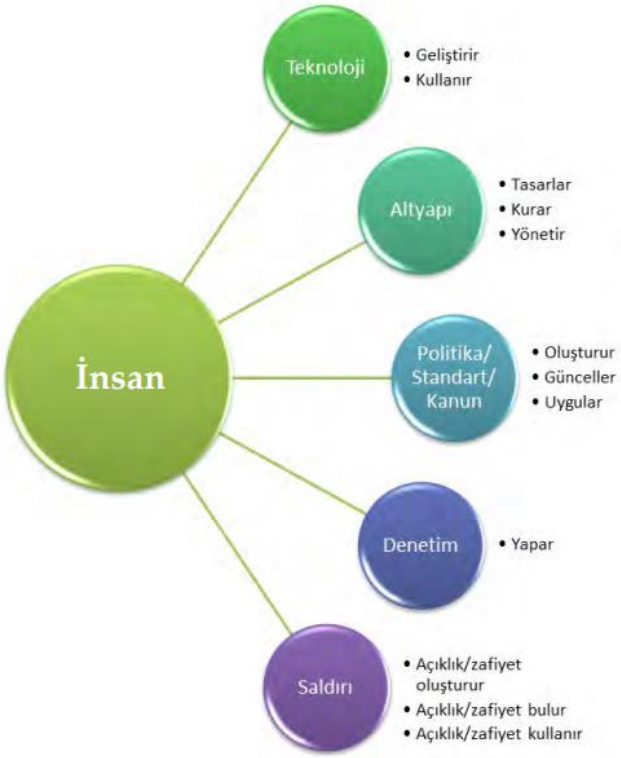
- Personelleri arasında planlı iş dağılımının yapılmaması,
- Personellerin görev tanımının açık bir şekilde yapılmaması,
- Personellere işe alım süreçlerinde gerekli eğitimin verilmemesi,
- Sorumluluğu kaldıramayacak kişilere yetkiler verilmemesi ve
- Olağanüstü durumlarda devreye girecek planlarının olmamasıdır.

Teknik Eksiklikler:

- Düzenli bir şekilde yedeklenmenin yapılmaması,
- Kurumların sahip oldukları teknolojilerin yetersiz olması,
- Verilerin uygun koşullarda depolanmaması ve
- Kurumların sahip olduğu teknolojilerin düzenli bir şekilde bakımlarının ve kontrollerinin yapılmaması olarak sıralanabilir.

İnsan Unsurundan Kaynaklanan Tehditler

Bilgi güvenliğinin sağlanmasında, doğal afetlere karşı önlemler alınıp ve kurumsallaşma yolunda tüm adımlar atılsa da sistemin en zayıf halkası olarak görülen insan unsurunun da dikkate alınması gerekmektedir (Puhakainen, 2006). Gün geçtikte insanlar, bilgi güvenliğinin gerçekleşmesi adına organizasyonların kurulması, teknolojinin yönetilmesi ve yasal düzenlemelerin oluşturulması gibi konularda etkin bir konuma gelmiştir (Erol ve Sağıroğlu, 2018). Bundan dolayı insan unsurundan kaynaklanacak bilgi güvenliği tehditleri tüm bilgi güvenliği sistemini olumsuz etkileyebilir. Araştırmalar, kurumlarda yaşanan bilgi güvenliği açıklarının birçok sebebinin insan davranışlarından kaynaklı olduğu belirtmişlerdir (ENISA, 2019; McAfee, 2019; The One Brief, 2020).



Şekil 1. Bilgi güvenliği sistemleri ile insan unsuru arasındaki ilişki (Erol ve Sağıroğlu, 2018)

Bireyler bilginin gizliliğini, bütünlüğünü ve ulaşılabilirliğini tehlikeye atabilmektedir. Alanyazında insan kaynaklı tehditler, bilinçli olan davranışlardan dolayı

doğan tehditler(kötü niyetli) ve bilinçli olmayan davranışlardan doğan tehditler(kazara) olarak ikiye ayrılmıştır (Colwill, 2009; Vural, 2007; Tekerek, 2008). Bilinçli olan davranışlardan doğan tehditler; kuruma öfkeli ve küs olan art niyetli çalışanların yetkilerini kötüye kullanmasından kaynaklı tehditlerdir. Bu tehditler yetkisi olmayan gizli bilgilere ulaşmak, kurum içi şifreleri kurum dışına çıkarmak, veritabanında yer alan verileri yok etmek ya da değiştirmek ve kasti olarak kötü yazılımların kurum bilgisayarlarına sızdırılması olarak sıralanabilir (Blanding, 2004). Mccue (2008), şirket veri ihlallerinin %70'inin dışardaki saldırıların aksine şirket içi çalışanlar tarafından gerçekleştirildiğini belirtmektedir. Bilinçli olmayan davranışlardan doğan tehditler ise yetersiz bilgi güvenliği eğitimlerinden ya da bilgi güvenliği farkındalığından kaynaklı bilginin gizlilik, bütünlük ve ulaşılabilirlik bileşenlerinin zarar görmesine sebep olabilecek tehditlerdir (Vural, 2007). Eminağaoğlu ve Gökşen (2009) insanların %70'lik kısmının bilgi güvenliği tehlikelerinden ve aldıkları sorumluluklardan habersiz olduklarını belirtmektedir. Bilinçli olmayan davranışlardan doğan tehditler; güvenlik politikalarına uymama, bilgi güvenliği farkındalığı eksiği, kişisel ve şirket bilgisayarlarının kullanılmadığı durumlarda açık bırakılması, hatalı yedekleme, gerekli olan yazılımların (anti virüs, güvenlik duvarı vb.) kullanılmaması ya da silinmesi, bilinmeyen adresten gelen e-postaların açılması, şifrelerin unutulması ve şifrelerin başkalarının erişebileceği fiziki ortamda saklanması olarak sıralanabilir (Canbek ve Sağıroğlu, 2006; Vural, 2007). Kurum ya da kişilerin bilgi sistemlerine sızabilmek için bireylerin davranışları izleyerek veri toplama sanatı olarak görülen sosyal mühendislik (Krombholz vd., 2015) günümüz bilgi güvenliği risk unsurları arasında önemli bir paya sahip olmaya başlamıştır. Sosyal mühendisler, sistemlere yönelik teknik saldırılar yerine sistemlere erişimi olan kişileri hedef almakta ve onları gizli bilgileri ifşa etmeye, ikna yoluyla kötü niyetli saldırılarını gerçekleştirmeye yönlendirmektedir. Teknik koruma önlemleri bu tür saldırılara karşı etkisiz olduğu (Krombholz vd., 2015) ve insanların bu saldırıları tespit etme konusunda zayıf oldukları görülmektedir (Qin ve Burgoon 2007). Sosyal mühendisler sıklıkla; güven uyandırmak, yardım istemek, yardım teklif etmek, sahte siteler oluşturup zararlı dosyalar göndermek ve suçluluk hissi yaratma gibi teknikler kullanmaktadır (Çek, 2017). Tüm bu durumlardan yola çıkarak insanların bilgi güvenliği farkındalığının eksik olması, gerekli önlemleri almamaları ve sahip olduğu sorumlulukların farkında olmamaları durumunda, insan unsurunun dahil olduğu tüm sistemlerin bilgi güvenliği tehditleriyle karşı karşıya kalması kaçınılmazdır.

2.1.3. Bilgi Güvenliğine Yönelik Tedbirler

Dijital dünyada bilgi güvenliğinin sağlanması kurumların kötü niyetli saldırılarının önüne geçmesi adına önem arz etmektedir. Ancak bilgi güvenliği sistemleri birçok bileşenden oluştuğundan dolayı sadece teknoloji temelli önlemler yeterli olmadığı görülmektedir (Tam vd., 2022). Bundan dolayı sağlıklı bilgi güvenliği, bilgi teknolojileri varlıkları ile etkileşim halindeyken bireylerin uyumlu davranışlarına bağlıdır. Bu tür davranışları etkileyen bilişsel faktörlerin araştırılması, etkili bir bilgi güvenliği politikasının tasarlanması adına önemlidir (Rhee vd., 2009). Bu bağlamda bilgi güvenliği sistemleri göz önünde bulundurulduğunda insan unsuru en önemli unsurlardan biridir ve bilgi güvenliğinin sağlanması ancak anti virüs sistemleri, güvenlik duvarları, yedekleme, kullanıcı eğitimleri ve farkındalık gibi bilgi güvenliğinin tüm halkasının tamamlanması ile mümkündür (Kılıç Aksu vd., 2015). Cherdantseva ve Hilton (2013) bilgi güvenliği sistemlerini, organizasyonel (strateji, politika vb.), teknolojik (güvenlik duvarı, anti virüs vb.), yasal (mevzuat, kanun vb.) ve insan (eğitim, farkındalık vb.) olarak dört ana başlıkta toplamıştır. Yine bu başlıkları destekler nitelikte Rao ve Nayak (2014), bilgi güvenliği sistemlerini insan, teknoloji ve organizasyon olarak üç başlıkta toplamıştır. Tüm bu bilgiler göz önünde bulundurularak bilgi güvenliğine yönelik tedbirler aşağıdaki şekilde sıralanmıştır;

Fiziki Unsurlara Yönelik Tedbirler

Fiziki unsurlardan kaynaklanan tehditlerin genellikle öngörülemeyen faktörlerden ortaya çıktığı görülmektedir. Bu tehditlere dair önlemler önceden programlanmalı ve gerçekleştirilmelidir (Güldüren, 2015). Fiziki unsurlardan kaynaklanan tehditler genellikle bilgi sistemlerinin tüm bileşenlerini etkilediği görülmekte ve sistemlerin çalışmamasına neden olmaktadır. Bu doğrultuda tehditlerin bilgi sistemlerine vereceği hasarı minimum düzeye indirgemek adına, kurumsallığa uygun eylem planları oluşturulmalı ve olası fiziki tehditlerden en kısa sürede nasıl kurtulabileceği ile alakalı kurum sürekliliğin sağlanması anlamında planlamanın önceden yapılması gerekmektedir (Blanding, 2004). Bunun dışında fiziki unsurlardan kaynaklanan tehditlerin başında gelen doğal afetlerden sonra bilgi kaybının yaşanmaması veya en aza indirilebilmesi için olası risklere karşı önlemler alınarak

düzenli olarak yedekleme işlemlerinin yapılması gerekmektedir. Bilgi sistemlerinin doğal afetlere karşı korunaklı şartlarda kurulması ve kurumsallığa uygun planlamaların yapılması tehditlerin vereceği hasarın en aza indirgenmesi adına faydalı olacağı düşünülmektedir (Uslu, 2007).

Teknolojik Temelli Tehditlere Yönelik Tedbirler

Bilgi güvenliği tehditleri genellikle teknolojik tedbirler kullanılarak çözülmeye çalışılmaktadır (Çavuşoğlu vd., 2009). Ancak kimlik doğrulama teknolojisi, güvenlik duvarları, sanal özel ağlar ve saldırı tespit sistemleri gibi geleneksel teknik çözümler bu sorunu tamamen çözmek için yeterli değildir. Bilgi güvenliğini sistemlerini tehlikelerden teknolojik temelli önlemlerle eksiksiz olarak korumak mümkün olmasa da donanımsal ve yazılımsal olarak alınacak tedbirler ile bilgi güvenliği sistemlerini belirli bir oranda güvende tutmak mümkündür (Gencer, 2015). Hem kişisel hem de kurumsal olarak teknolojik temelli tedbirler;

- Şifreleme Teknolojileri,
- Yedekleme,
- Sayısal(dijital) İmza,
- Anti virüs yazılımları,
- Güvenlik Duvarı,
- Yazılım güvenliği
- Kullanıcı hesabı güvenliği ve
- Ağ güvenliği olarak sıralanmaktadır (Özenç, 2007).

Bu önlemlere ek olarak, yazılımların güncel tutulması, kullanılmayan uygulamaların kaldırılması ve şifre kurallarına uyulması önerilmektedir.

Organizasyonel Tehditlere Yönelik Tedbirler

Bilgi güvenliği sistemlerinin yönetimi, güvenlik politikalarının belirlenmesi, plan ve stratejilerin standartlara uygun şekilde uygulandığı durumlarda sağlanabilir. Organizasyonel

tedbirler kurum işleyiş sürecinin bir parçasıdır. Doğru program, politika ve stratejilerin gerçekleştirilmesi başlıca organizasyonel tedbirlerdir. Organizasyonel anlamda yapılan ve yapılması gereken tedbirler şu şekilde sıralanabilir;

Bilgi Güvenliği Politikalarının Kullanılması: Bilgi güvenliğinin sağlanmasında bilgi güvenliği politikaları önemli bir rol oynamaktadır (Dhillon, 2017). Bilgi güvenliği politikaları, kurum çalışanlarının ve yöneticilerinin belirli sorumluluklara ve uyması gereken prosedürleri ifade etmektedir (Rees vd., 2003; Siponen ve Vance, 2010). Kurumlar bilgi güvenliği politikaları oluşturarak bilginin olası tehditlerden korunmasının önüne geçmeyi hedefler. Birçok kurum bilgi güvenliği politikalarının oluşturmak için ISO/IEC 27001 standardını temel almaktadır (Kang vd., 2022). İlk olarak 1998'de İngiltere'de yayınlanan Uluslararası Standartlar Kurumu (ISO) tarafından kabul edilen ISO/IEC 27001 ülkemizde ise Türk Standartlar Enstitüsü (TSE) tarafından 2002 yılında kabul edilmiştir. Dünya genelinde kabul gören ISO/IEC 27001 standardı bilgi güvenliğinin üç bileşeni olan gizlilik, bütünlük ve ulaşılabilirlik bileşenlerine yönelik tehditlerinin önlenmesine yönelik politikalara temel olmaktadır.

Güvenlik Komitesinin Oluşturulması: Kurumlar için bilgi güvenliğinin sağlanması adına önemli tedbirlerden bir tanesi güvenlik komitesi oluşturulmasıdır. Tüm dünyada kabul gören ISO/IEC 27001 standardının gerekli gördüğü güvenlik komitesi oluşturulması bilgi güvenliğinin sağlanmasında önemli bir unsurdur (ISO, 2022). Oluşturularak olan güvenlik komitesinin görevleri şu şekildedir;

- Kurum misyonunu, işin sürekliliğini bozacak bilgi güvenliği tehditlerine karşı yapılması gereken önlemlerin belirlenmesi,
- Güvenlik politikalarına uyumun sağlanması,
- Kurum politikalarıyla uyumlu bilgi güvenliği sistem yönetim modelinin oluşturulması (International Organization for, 2020).

Bilgi Güvenliği Kültürünün Oluşturulması: Alhogail (2015) bilgi güvenliği kültürünü, bilgi güvenliğinin sağlanması adına bilgi güvenliği sistemleriyle insan etkileşimini etkileyen algı, tutum ve varsayımlar olarak tanımlamaktadır. Bilgi güvenliği

kültürü, kurumlardaki bilgi güvenliği sistemi tehlikelerinin önlenmesi adına bilgi teknolojilerinin kullanımı ile ilgili bireylerin davranışlarına kılavuz oluşturmaktadır. Bilgi güvenliği kültürünün oluşması adına, kurumun bilgi güvenliği konusunun önemine inancının olması, bilgi güvenliği politikalarının belirlenmesi ve çalışanların bilgi güvenliği davranışlarının gelişmesi adına motive ve teşvik edilmesi gibi konuların sağlanması gerekmektedir (Helokunnas ve Kuusisto, 2003). Bu bağlamda oluşturulacak bilgi güvenliği kültürünün kurumların bilgi güvenliğini ve kurum çalışanlarının bilgi güvenliğine yönelik davranışlarını etkilediği belirtilmektedir (Veiga ve Eloff, 2010). Bunun yanı sıra kurumların organizasyonel tehditlere yönelik aldığı tedbirler, her ne kadar tehditlerin bir bölümünü önüne geçse de ülkelerin yasal anlamda kurumları ve bireyleri güvende tutmak adına yasal tedbirler alması gerekmektedir. Bundan dolayı organizasyonel tehditlere yönelik alınan tedbirlere ek olarak yasal tedbirlerde gün geçtikçe ortaya çıkmaktadır.

İnsan Unsuru Kaynaklı Tehditlere Yönelik Tedbirler

Son dönemde artan teknolojinin uygunsuz kullanımı ile birlikte bireylerin bilgi güvenliği farkındalık düzeylerinin düşük olması, bireyleri birçok bilgi güvenliği tehdidiyle karşı karşıya bırakmaktadır. Bu bağlamda bilgi güvenliğini sağlamak amacıyla çok sayıda teknolojik temelli önlem alınsa da bilgi güvenliği tehditlerinin tam olarak bittiği söylenemez (Pahnila vd., 2007). Alanyazında, kurumlarda bulunan teknoloji temelli önlemlerin gücü ne kadar olursa olsun, bilgi güvenliğinin en zayıf halkası olarak tanımlanan insan unsurunun göz ardı edilmesinden kaynaklı saldırıların daima gerçekleşeceğini savunmuşlardır (Abawajy, 2014; Arce, 2003; Jansson ve von Solms, 2013). Dünyada insan odaklı bilgi güvenliğinin sağlanması adına bilgi güvenliği eğitimi önemli rol oynamaktadır. (Chou ve Chou, 2016; Hadlington, 2017; Li vd., 2019). Bu bağlamda bilgi güvenliğine yönelik tehditlerin en aza indirilmesi konusunda insanlara çeşitli görevler düşmektedir. Tüm verilerden yola çıkarak insan odaklı alınacak tedbirler ise şu şekilde sıralanabilir;

Bilgi Güvenliği Farkındalığı Oluşturma: Teknolojiyle iç içe olmanın kaçınılmaz olduğu günümüz dünyasında bireyler bilgi güvenliği kavramıyla karşı karşıya gelmektedir. Bireyler bilgi güvenliği sistemlerinin en zayıf zinciri halini almış ve bu anlamda bilgi

güvenliği farkındalığının kazandırılması hayati önem kazanmıştır (Kritzinger ve Smith, 2008; Mart, 2012; Veiga, 2008). İnsan kaynaklı oluşan bilgi güvenliği tehditlerinin insanların kötü niyetinden ziyade bilgi güvenliği farkındalık düzeylerinin düşük olmasından kaynaklandığı görülmektedir (Parsons vd., 2014). Bu anlamda çalışanın bilgi güvenliği farkındalığı eksikliğinden kaynaklanan riskleri minimuma düşürebilmek adına eğitim ve farkındalık çalışmalarının gerçekleştirilmesi önem arz etmektedir. Türkiye'de bilgi güvenliği farkındalığı sağlanmasına yönelik üniversite, kamu kurum ve kuruluşlarının düzenlendiklerini seminerler, bakanlık ve kurumların el broşürü, duvar ilanları veya kamu spotlarının yayınlanması ve gönüllüler tarafından oluşturulmuş çevrimiçi öğretim materyalleri aktif olarak kullanılmaktadır.

Ebeveyn Kontrolü İle Alınacak Tedbirler: Çevrimiçi ortamda karşılaşılması olası tüm tehditlerin çıkış noktası gerçek hayattaki tehditlerdir. Bu bağlamda ebeveynler gerçek hayattaki tehditlerden çocuklarını korumak için ne kadar çaba harcıyorsa çevrimiçi ortamda da bu tehditlere karşı gerekli çabayı göstermesi gerekmektedir. Ebeveynlerin çevrimiçi tehditlere karşı bilgi sahibi olmaları, riskleri azaltabilir ve güvenli bir ortam sunabilir (BTK, 2019). Şendağ ve Odabaşı (2006) tarafından ebeveyn kontrolü ile ilgi bazı önerileri aşağıda sunulmuştur:

- Çocukların kişisel bilgilerini paylaşacağı çevrimiçi herhangi bir sayfada mutlaka ebeveynlerden izin almaları,
- Ebeveynlerin izni olmadan bilgisayara yazılım yüklenmemesi,
- Çevrimiçi ortamda tanıştığı kişiler ile ebeveynlerinin bilgisi olmadan buluşmamalı,
- Çevrimiçi ortamda adres ve anlık konum bilgilerinin verilmemesi,
- Ebeveynlerinden habersiz sosyal ağ platformlarına kaydolmamaları,
- Ebeveynlerin izni olmadan çevrimiçi ortamda fotoğraf veya e-posta göndermemeleri,
- Ebeveynlerin izni olmadan e-ticaret sitelerinden alışveriş yapmamaları ve
- Farkında ya da farkında olmadan çevrimiçi ortamda karşılaştıkları her türlü tehdit unsuru içeriği ebeveynleri ile paylaşılması gerektiği iletilmelidir.

Bu anlamda ebeveynler çevrimiçi ortamdaki kuralları çocuklarıyla birlikte koyarak çocukların çevrimiçi tehditler hakkındaki farkındalığının artmasında etkili rol oynamaktadır (Kuzu, 2008).

Sosyal Medya Platformlarında Alınacak Tedbirler: Her geçen gün hızla artan sosyal medya kullanıcı sayısının 4.200 milyara yükseldiğini ve dünya nüfusunun %53.6'sının sosyal medya kullanıcısı olduğunu yapılan araştırma raporlarında ortaya konulmaktadır (bkz., Statista, 2022; SimilarWeb, 2022). Günümüzde sosyal medya kullanımı toplumun belirli bir kesmi ile sınırlı kalmayarak çocuklar dahil olmak üzere herkesin hayatına girmiştir (Rasheed vd., 2020). Çevrimiçi teknolojileri çok sık ve kontrolsüz bir şekilde kullanmak, bireylerin bilgi güvenliğini tehlikeye atmakta ve birçok riske maruz kalmasına neden olmaktadır (Abaido, 2020). Özellikle erken yaşta teknoloji ile buluşan çocuklar yine bu risklerle erken yaşta karşı karşıya kalabilmektedir. Hızla çeşitlenerek yaygınlaşan sosyal medya araçları da özellikle çocuklar başta olmak üzere tüm kullanıcıları tehdit eden çevrimiçi saldılar için yeni fırsatlar doğurmuş ve bilgi güvenliğine yönelik sorunlarla karşı karşıya kalmalarına neden olmaya başlamıştır. İnsanların günlük yaşamının her alanında çevrimiçi ortamlar ve mobil teknolojilerle iç içe olması nedeniyle bu konuyla ilgili tedbirlerin gecikmeden alınması gerektiği düşünülmektedir (Güldüren vd., 2016). Bu çerçevede Şenol ve Karacan (2012) tarafından sosyal medya platformlarında bilgi güvenliğini sağlamak amacıyla alınacak önlemler aşağıda sunulmuştur;

- Bilgisayarda bulunan yazılımları güncel tutmak
- İşletim sistemini güncel tutmak
- Gelen e-postalara karşı temkinli olmak
- Şifrelerin belirli aralıklarla yenilenmesi
- Sosyal medya platformlarını kullandıktan sonra "çıkış" yapmak
- Güvenilmeyen cihazlardan kullanıcı girişi yapılmaması
- Kişisel bilgiler herkese açık şekilde paylaşılmaması

Yasal Tedbirler

Günümüzde birçok kurum ve kuruluş bireylere hizmet vermek amacıyla çoğunlukla bireylerin rızasına veya bir sözleşmeye dayanarak kullanıcıların kişisel bilgilerini toplamaktadır (Vural, 2017). Vatandaşların temel hak ve özgürlüklerinin ihlal edilmesi, insanların kişisel verileri üzerinden haksız kazanç sağlanması ve insanların kişisel verilerinden dolayı mağdur olması gibi faktörlerden dolayı ülke yöneticileri tarafından kurumları ve bireyleri koruyacak yasal tedbirlerin alınması kaçınılmaz olmuştur (Korkmaz, 2017). Ülkemizde bilgi güvenliğine yönelik alınan yasal tedbirler şu şekildedir:

Kişisel Verilerin Korunumuna Dair Yasal Tedbir: Kişisel verilerin korunması kanununa (KVKK) göre kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi; kişisel verilerin işlenmesi ise kişisel verilerin veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, aktarılması ve elde edilebilir hale getirilmesi gibi veriler üzerinde gerçekleşen her türlü işlemi" ifade etmektedir (KVKK, 2016). KVKK'nin temel amacı "kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir" (KVKK, 2016). Kanun içeriğinden anlaşılacağı üzere ad, soyad, kimlik numarası, adres bilgileri, banka hesap numaraları, şifreler vb. veriler kişisel veri olarak tanımlanmakta olup kanun ile korunmaktadır. 2010 yılında 5982 sayılı kanunla yapılan Anayasa değişikliği ile Anayasanın 20. maddesine bir fıkra eklenerek "özel hayatın gizliliği ve korunması hakkı" kapsamında kişisel verilere Anayasal güvence altına alınmıştır. Bu fıkra; "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." şeklindedir (KVKK, 2016). Bu anlamda insanlar kişisel verilerinin korunumu ve bu verileri izinsiz bir şekilde üçüncü şahısların eline geçmemesi konusunda yasal tedbirler ile korunmaktadır.

Elektronik Haberleşme Kanunu: Elektronik haberleşme sektörünü düzenleyen 5809 sayılı kanunun 12. maddesinde kurumlara: kişisel veri gizliliği ve korunması, yetkisiz erişime karşı gerekli önlemlerin alınmasına yönelik sorumluluklar getirmiştir (Mevzuat, 2022). Esas madde olan 51. maddenin 1. fıkrasında "Kişisel verilerin işlenmesinde; hukuka ve dürüstlük kurallarına uygun olması, doğru ve gerektiğinde güncel olması, belirli, açık ve meşru amaçlar için işlenmesi, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ile işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi ilkelerine uyulur." kanunu ile kişisel verilerin korunmasına yönelik net yükümlülükler getirilmiştir.

2.2. Görev Temelli Öğrenme

Görev kavramı, farklı insanlar için farklı anlamlar taşımakta olup alanyazında fikir birliği olmamakla birlikte çeşitli tanımlar yapılmıştır. Görev temelli öğrenmenin ilk savunucularından biri olan Prabhu'ya (1987) göre görev; öğrencilerin bir düşünce süreci yoluyla verilen bilgilerden bir sonuca ulaşmasını gerektiren ve öğretmenlerin kontrol etmesine ve düzenlemesine izin veren bir etkinlik sürecidir. Long (1985) ise çalışmasında görevi, bireyin kendisi veya başkaları için özgürce veya bir ödül için yaptığı bir eylem olarak tanımlamıştır. Willis'e (1996) göre ise görev, öğrencilerin bir problem çözme ve deneyimlerini paylaşma gibi gerçek bir sonuca ulaşmak için dil unsurunu kullandıkları bir aktivedir. Genel olarak alanyazında yapılan çalışmalar incelendiğinde temel olarak görev; yeni bir dilde yetkilendirilen bilgi ve yeteneklerin iyileştirilmesi ve iletişim sırasında kullanılması için fırsatların sağlanması için yapılandırılmış bir plan olarak tanımlanmaktadır (Ellis, 2003). Bir etkinliğin görev olup olmadığı anlamak için ise genel olarak aşağıdaki sorulara cevap aranmaktadır.

- Etkinlik öğrencilerin ilgisini çekiyor mu?
- Bir sonuç var mı?
- Başarı sonuca göre mi değerlendiriliyor?
- Görev gerçek dünyadaki eylemler ile ilgili mi? (Willis ve Willis, 2007).

Bu bağlamda görev örnekleri arasında bir çiti boyamayı, bir kişiyi bilgilendirmeyi ya da ortaya bir ürün koymayı gösterebiliriz. Bir başka deyişle görev, insanların günlük yaşamda, okulda, işte yaptığı eylemleri kastetmektedir. Görev temelli öğrenme hedef, girdi, yöntem, rol ve düzenleme olarak beş bileşenden oluşmaktadır (Nunan, 2004).

- Hedef: Herhangi bir öğrenme görevinin arkasındaki belirsiz, genel hedefleri ifade etmektedir. Görev ile müfredat arasında bir bağlantıyı sağlamaktadır.
- Girdi: Öğrencinin bir görevi tamamlama sürecinde çalıştığı sözlü, yazılı ve görsel verileri ifade etmektedir.
- Prosedür: Öğrencilerin bir görevinin girdisiyle nasıl başa çıktıklarının yollarını ifade etmektedir.
- Rol: Öğrencilerden görevlerini yerine getirme aşamasında yapması beklenen eylemleri ifade etmektedir.
- Düzenleme: Görevde belirtilen düzenlemelerini ifade etmektedir.

Bu doğrultuda görevlerin seçilmesi, değiştirilmesi ve oluşturulmasında tüm bu bileşenlerin göz önünde bulundurulması önem arz etmektedir (Nunan, 2004).

2.2.1. Görev Temelli Öğrenmenin Dayanağı

Görev temelli öğrenme sağlık bilimlerinde olduğu gibi uygulamalı bilimlerde de aktif olarak kullanılan bir öğrenme yöntemidir (Harden vd., 1996). Görev temelli öğrenmenin çeşitli avantajları olduğu ve bu ortamın öğrenci odaklı olması nedeniyle geleneksel yöntemlere göre daha etkili ve verimli olduğu söylenebilir. Görev temelli öğrenmenin geleneksel yönteme göre avantajları tablo 1'de sunulmuştur.

Tablo 1

Görev temelli öğrenmenin avantajları

Avantaj	Açıklama
Durumlu Öğrenme	Geleneksel öğrenme yönteminin durumsuz olduğu ancak görev temelli öğrenmenin hem durumlu hem durumsuz olduğu görülmektedir (Brown vd., 1989). Bu anlamda görev temelli öğrenmede gerçekleştirilen görevler sonrası ortaya çıkan bilgilerin genelleştirilebilir bilgi olduğu görülmektedir (Akyüz, 2012).
Zorluk Düzeyi	Hazırlanan görevlerin öğrencilerin hazırbulunuşluk seviyelerine göre hazırlanması gerekmektedir. Eğer görevler öğrencilerin gerçekleştiremeyeceği kadar zor olursa öğrencilerin görevi tamamlayamamasına ve sonraki görevlere olan ilgisinin düşmesine sebep olabilir. Aksi durumda ise öğrencinin dersi kolay ve önemsiz görmesine neden olabilir. Bu öğrenme ortamında ise hafta hafta farklı zorluk düzeyinde görev verilebilmektedir.
Tecrübeyle Öğrenme	Görev temelli öğrenme ortamında görevlerin gerçek hayatı temsil eden etkinliklerden tercih edilmesi nedeniyle öğrenenlerin görevleri deneyimleyerek öğrenmesi mümkün olmaktadır.
Motivasyon	Öğrenen yeteri kadar motivasyona sahip değilse beklenen verimi vermeyeceği olası görülmektedir. Öğrenme sürecinin görevler üzerinden sağlanması ve görev sonrası başarma duygusu nedeniyle öğrenen motivasyonlarının kalıcı olarak artacağı düşünülmektedir. Ayrıca, görev temelli çevrimiçi öğrenme ortamında motivasyonlarını yüksek tutmak ve verimlerinin düşmemesi adına ödül sistemi kullanmanın uygun olacağı düşünülmüştür.

2.2.2. Görev Türleri

Görev türlerini sınıflandırmanın genel olarak kabul edilmiş bir yolu bulunmamaktadır. Genel olarak görev türleri belirlenirken öğrencilerin görevleri gerçekleştirirken yürütmeleri gereken işleyiş açısından pedagojik unsurlar dikkate alınmaktadır (Ören, 2021). Willis ve Willis (2007) yaptıkları görev tür sıralanmasını bilişsel süreçleri dikkate alarak yaptıklarını ve bu türlerin kullanılması konusunda öğretmenler için bir araç olma noktasında belirgin ve üretici bir sıralama olduğunu ifade etmektedir. Konuyla ilgili Willis ve Willis (2007) aşağıdaki gibi yedi görev türünden söz etmektedir. Bunlar;

- Listeleme: Diğer görev türlerinden daha basit olduğundan en çok tercih edilen görev türüdür. Bu görevler, öğrenciler fikirlerini açıklamaya çalışırken birçok konuşma ortamı yaratır. Listeleme görevleri sırasında beyin fırtınası ve gerçeği bulma olarak iki süreç aktif olmaktadır. Beyin fırtınası, çekingen öğrencileri

konulara dahil eder ve daha zengin görev etkileşimini teşvik eder. Gerçeği bulma ise öğrencilerden kitaplar veya broşürler gibi farklı kaynaklarda veya çevrimiçi ortamda belirli gerçekleri aramalarını bekler.

- Sıralama ve ayırma: Bu görev türünde, çeşitli bilişsel süreçler yer alır: bir hikaye oluşturmak için bir dizi karışık resmi düzenlemek veya belirli bir sürecin adımlarını sırayla tanımlamak gibi öğeleri, eylemleri veya olayları mantıksal veya kronolojik bir sıraya koymak olabilmektedir.
- Eşleştirme: Bu görev türünde, seviyeleri ne olursa olsun tüm öğrenciler için uygundur. Bu görevler okuma, yazma ve dinlemeyi içerecek şekilde uyarlanabilir. Eşleştirme içeren görevleri kullanmanın büyük bir avantajı, öğrencilerin sıkı ve iyi tanımlanmış bir çerçevenin güvenliği içinde göreve çok zengin bir şekilde maruz kalmalarıdır.
- Karşılaştırma: Bu görev türü, benzerlikleri veya farklılıkları bulmak için öğrencilerin sahip oldukları ve farklı kaynaklardan aldıkları bilgileri karşılaştırmayı içermektedir.
- Problem çözme: Bu görev türü, öğrencinin düşünme ve tartışma gücüne ihtiyaç duyulduğundan çözülmesi zor ve tatmin edicidir. Problem çözme görevleri, öğrencileri küresel ısınma gibi genel sorunlar için tavsiye ve öneriler bulmaya teşvik etmektedir. Bu görevler, geniş kapsamlı tartışmaya teşvik edebilir, bunun yanında not alma, taslak hazırlama ve çözüm önerilerini sonuçlandırma dahil olmak üzere çeşitli yazma etkinlikleri için ön ayak olabilir.
- Paylaşım görevleri: Bu görevler, öğrencilere kendileri hakkında özgürce konuşma ve deneyimlerini sınıfta başkalarıyla paylaşma şansı verir. Deneyimler anlatılırken, öğrenciler konuşmacılara sorular sormak, hafıza testleri hazırlamak veya hikayeyi yeniden anlatmak için notlar alabilirler.
- Yaratıcı görevler: Bu görev türünde ise öğrenci işbilirliği içerisinde yapması gereken görevleri ifade etmektedir. Görev sonucunda ortaya bir ürün çıkması beklenmektedir.

Tüm bu görev türleri göz önünde bulunudurulduğunda öğrenme ortamının zengin ve etkileşimli görevler ile hazırlanması durumunda öğrenci başarısının ve motivasyonunun artabileceği söylenebilir. Görev temelli çevrimiçi öğrenme ortamının daha çok dil odaklı çalışmalarda kullandığı görülmektedir (Akyüz, 2012). Görev temelli çevrimiçi öğrenme ortamının en büyük avantajı, öğrencilerin sahip oldukları yetenekleri kullanma olanağı sunması, ürün odaklı ve gerçek hayat etkinliklerini içermesidir (Pools-m, 2013). Bu yöntem öğrenenin bilgi ve becerilerini süreç boyunca aktif bir şekilde kullanması, pratik yapması ve öğrenenin sonuca odaklı eğitim görmesi açısından önemlidir. Bunun yanı sıra öğrenme ortamında bulunan görevler öğrencilerin motivasyonlarının yüksek tutulması hedeflenmesi sebebiyle Newcomb ve Treftz (1987) tarafından geliştirilmiş olan yaklaşım temel alınmıştır. Her hafta öğrencilere çok kolay, kolay, zor, çok zor zorluk seviyelerinde görevler tanımlanmıştır. Bu bağlamda öğretici, öğrencilerin hedeflere ne ölçüde ulaştığını tespit edebilir ve öğrenciler problem çözme yeteneklerini geliştirebilir.

2.3. İlgili Araştırmalar

Bu bölümde bilgi güvenliğine ve görev temelli öğrenme ortamına yönelik alanyazındaki ilgili araştırmalara yer verilmiştir.

2.3.1 Bilgi Güvenliğine Yönelik Araştırmalar

Yoon vd., (2012) yaptıkları çalışmada, üniversite öğrencilerinin bilgi güvenliği davranışlarını motive eden faktörleri incelemiştir. Çalışmada koruma motivasyon teorisi isimli teori benimsenmiştir. Öğrencilerin bilgi güvenliği davranışlarını değerlendirmek için sosyal normları ve alışkanlıkları modele entegre edilmiştir. 202 kişinin katılım gösterdiği çalışmada ciddiyet, yanıt verme becerisi ve öz yeterlilik algı seviyesi yüksek olan öğrencilerin bilgi güvenliği davranışlarını uygulama konusunda daha fazla motive oldukları görülmüştür. Koruma motivasyon teorisinin, öğrencilerin bilgi güvenliğine yönelik tutumlarını belirleme adına önemli bir teori olduğunu ve motivasyonlarının bilgi güvenliği farkındalığı eğitimlerinden etkilendiklerini öne sürmüştür.

Kim (2014) yaptığı çalışmada, bilgi güvenliği farkındalığı eğitimi geliştirmek adına üniversite öğrencilerinin bilgi güvenlik farkındalığı durumlarını araştırmıştır. Çalışma sonucunda üniversite öğrencilerinin çoğunluğunun bilgi güvenliği farkındalığı eğitiminin gerekliliğinin farkında olduğunu tespit etmiştir. Aynı zamanda öğrencilerin güvenlik kavramlarını çeşitli kaynaklardan parça parça öğrendiği görülmüştür.

Kajzer D'Arcy vd., (2014) yaptıkları çalışmada, bilgi güvenliği farkındalık yöntemlerinin kişilik özelliklerine göre farklı tipteki bireyler için etkili olup olmadığını incelemişlerdir. 293 kişinin katılım gösterdiği anket sonrası bilgi güvenliği farkındalık yöntemlerinin kişiliğe göre değişiklik gösterdiğine ancak her zaman bu şekilde olmadığı sonucuna varmışlardır.

Güldüren (2015), yükseköğretim kurumlarında çalışan öğretim elemanlarına bilgi güvenliği farkındalığını kazandırmaya yönelik 363 öğretim elamanın katılım gösterdiği çalışmada bilgi güvenliği farkındalığı ölçeği geliştirmiştir. Geliştirilen ölçek sonrası 31 deney grubu, 34 kontrol grubu olmak üzere toplam 65 öğretim elemanının bulunduğu çalışma grubu üzerinde 12 hafta süren yarı deneysel süreç gerçekleştirmiştir. Gerçekleştirilen deneysel süreç sonrasında deney ve kontrol grubundaki öğretim elemanları bilgi güvenliği farkındalık düzeyleri arasında anlamlı bir farklılık olduğu görülmüş ve araştırmacı tarafından geliştirilen çoklu ortam materyalleri ile web sitesinin deney grubu öğrencilerinin bilgi güvenliği farkındalık düzeyi toplam puanlarını artırdığı belirlenmiştir.

Stanciu ve Tinca (2016) yaptıkları çalışmada, muhasebe mesleğinin her alanına bilişimin dahil olması gerektiğini öne sürerek muhasebe öğrencilerinin bilgi güvenliği farkındalıklarını incelemiştir. Çalışma öğrencilerin bilgi işlem bilgilerinin daha teknik anlamda olduğunu ve bilgi güvenliği konusunda eksik olduklarını gözlenmiştir. Bu bağlamda öğrencilerin bilgi güvenliği farkındalık kazandırılması konusunda üniversitelerin müfredatının acilen iyileştirilmesi gerektiğini öne sürmüşlerdir.

Güldüren vd., (2016) yaptıkları çalışmada, ortaöğretim kurumlarında öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek

geliştirmiştir. Araştırma 607 öğrenci üzerinde gerçekleştirilmiştir. Yapılan analiz sonucunda ölçeğin 36 madde ve 3 alt boyuttan oluştuğunu ve ölçeğin tamamı için Cronbach's Alpha güvenirlik katsayısını ,955; her alt boyut için sırasıyla saldırı ve tehditler: ,954, mahremiyet: ,890 ve kişisel verilerin korunması: ,808 olarak bulunmuştur. Ayrıca çalışma sonucunda ortaöğretim kurumlarındaki öğrencilerin bilgi güvenliği farkındalık düzeyleri ile cinsiyetleri arasında anlamlı bir farklılığın olduğunu tespit etmişlerdir.

Çetinkaya vd., (2017), öğretmenlerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik 516 öğretmenin katıldığı ölçek geliştirme çalışması sonucunda üç faktör altında ("Mobil cihazlar, Mahremiyet ve İletişim", "Saldırı ve Tehditler" ve "Genel Güvenlik") 48 maddeden oluşan bir ölçek geliştirmiştir. Geliştirilen ölçeğin tamamı için Cronbach's Alpha güvenirlik katsayısını ,980; her alt boyut için sırasıyla Mobil cihazlar, Mahremiyet ve İletişim: .967, Saldırı ve Tehditler: ,969 ve Genel Güvenlik: ,926 olarak bulunmuştur.

Mccormac vd., (2017) yaptıkları çalışmada, bireylerin bilgi güvenliği farkındalığı düzeyleri ile yaş, cinsiyet, kişilik ve risk alma eğilimi gibi bireysel farklılık değişkenleri arasındaki ilişkiyi incelemiştir. 505 kişiye uygulanan anket sonrasında ortaya çıkan sonuç bireylerin vicdanlı olma, uyumlu olma, duygusal istikrar ve risk alma eğilimi değişkenlerinin bireylerin bilgi güvenliği farkındalıklarını önemli ölçüde açıkladığını ancak yaş ve cinsiyetin değişkenlerinin açıklamadığını tespit etmişlerdir.

Ki-aries ve Faily (2017) yaptıkları çalışmada, bireyleri bilgi güvenlik farkındalık uygulamasına dahil ederek güvenlik ile bağlantılı insan faktörlerini belirlemeyi amaçlamıştır. Çalışma sonucunda birey merkezli bilgi güvenliği farkındalığı yaklaşımının, iş süreçleri içerisinde dahil edilmesi adına gerekli zamana ve kaynağa uyum sağlayabileceğini ve bu yaklaşımın bilgi güvenliği risklerini azaltmaya yönelik olumlu bir katkı sunduğunu tespit etmişlerdir.

Parson vd., (2017) yaptıkları çalışmada, bilgi güvenliği farkındalığının bir kuruluşu siber tehditlerden korunmanın ayrılmaz bir parçası olduğunu öne sürmüştür. Bilgi güvenliği

farkındalığını ölçmek için bilgi güvenliği konulu anket çalışması yapılmıştır. 505 öğrencinin katılım gösterdiği çalışma sonucunda bilgi güvenliği puanları yüksek olan öğrencilerin bilgi güvenliği tehditlerine karşı daha fazla duyarlı olduğu sonucu ortaya çıkmıştır.

Sinha vd., (2019) yaptıkları çalışmada, bilgi güvenliği tehditleri ve saldırıları hakkında ayrıntılı bir çalışma ortaya koymuşlardır. Bilgi güvenliği tehditlerini ağ, sunucu ve uygulama ana başlıkları altında incelemişlerdir. Mevcut çözümlerin belirli bir saldırı türünü hedef aldığını ve kişisel bilgilerin korunması için genel güvenlik çözümlerinin yeterli olmadığını bu önlemlerin geliştirilmesi gerektiğini savunmuşlardır.

Van der Schyff ve Flowerday (2021) yaptıkları çalışmada, bilgi güvenliği farkındalık düzeyinin facebook gizlilik ayarlarını gözden geçirme davranışlarına etkisini ve beş büyük kişilik özelliklerinin arasındaki ilişkileri incelemişlerdir. 594 kişinin katılım gösterdiği çalışma sonucunda, bilgi güvenliği farkındalığının aracı bir görev gördüğünü ancak yalnızca bazı kişilik özellikleri için bu durumun söz konusu olduğunu ortaya koymuşlardır.

Wu vd., (2021) yaptıkları çalışmada, bilgi güvenliği eğitiminin öğrencilerin bilgi güvenliği farkındalığını geliştirmek için etkili bir yöntem olacağını fakat bu alanda çalışmaların yeterli olmadığını belirtmiştir. Bu doğrultuda çalışmada, oyunlaştırma stratejisi benimsenerek öğrencilerin bilgi güvenliği farkındalıklarının gelişim düzeyleri ve oyunlaştırılmış öğrenme ortamının cinsiyet değişkeni arasındaki farkı da incelemişlerdir. Çalışma sonucunda oyunlaştırılmış sınıftaki öğrencilerin geleneksel yöntem ile öğrenim gören öğrencilerden bilgi güvenliği davranışı konusunda daha iyi performans ortaya koyduğu ve öğrenme ortamının bilgi güvenliği farkındalığını arttırma üzerinde cinsiyet arasında fark olmadığı sonucuna ulaşılmıştır.

Solomon vd., (2022) yaptıkları çalışmada, kullanıcıların bilgi güvenliği farkındalığını değerlendirmek adına bağlam temelli, veriye dayalı yeni bir yaklaşım kullanmışlardır. 120 akıllı telefon kullanıcısının katılımıyla değerlendirilen yaklaşım sonucunda bağlam temelli veriye dayalı yaklaşımın bireylerin bilgi güvenliği farkındalığını değerlendirme anlamında güvenirliğini önemli ölçüde iyileştirdiğini belirtmiştir.

2.3.2. Görev Temelli Öğrenme Ortamına Yönelik Araştırmalar

Lee (2002) yaptığı çalışmada, öğrencilerin iletişim becerilerini geliştirmek için görev tabanlı strateji ile elektronik sohbetleri kullanan bir pilot çalışmayı incelemiştir. Görev tabanlı stratejinin, gerçek hayattaki konularda iki yönlü bilgi alışverişine odaklandığını belirtmiştir. Öğrenciler, dil öğrenme sürecinde öğrenimin sağlanması ve işbirliği için farklı işlevsel becerilere erişmeleri gerektiğinden, çevrimiçi görev tabanlı etkinliklerden yararlanmıştır. Araştırma sonucunda, çevrimiçi iletişimin dil öğrenme süreci üzerinde önemli bir etkisi olduğunu tespit etmiştir ve yabancı dil eğitimcilerinin özellikle öğrenen-öğreten etkileşimi sırasında öğrencilerin fikir üretimini engellediğinin farkında olmaları gerektiğini öne sürmüştür.

Akyüz (2012) yaptığı çalışmada, görev temelli çevrimiçi öğrenme ortamının öğrencilerin motivasyonlarına, bilişsel yüklenmelerine ve problem çözme becerisi algılarına etkisini araştırmıştır. Dört hafta süren deneysel süreçte görev temelli öğrenme yaklaşımı benimsenerek hazırlanan ortamda her hafta kısa bir ders anlatım sunusu eğitsel ajan tarafından öğrencilere verilmiş ve dersin sonunda haftanın görevi verilmiştir. Deneysel süreç sonucunda uygulanan yöntemde arkadaş rolünde hazırlanan ajandan eğitim gören öğrenenlerin eğitsel ajan öğrenenlerine göre motivasyonlarının daha yüksek olduğu görülmüştür. Görev temelli çevrimiçi öğrenme yönteminin öğrenenlerin problem çözme becerisi algısı üzerinde anlamlı bir farklılık olduğu tespit edilmiştir.

Herath vd., (2013) yaptıkları çalışmada, öğrencilerin siber saldırıları önlemek için güvenlik protokolleri, algoritmaları ve web uygulamalarını anlamalarına yardımcı olacak bir görev temelli aktif öğrenme ortamı geliştirmişlerdir. Geliştirilen aktif öğrenme ortamı bilgi teknolojileri, mühendislik ve işletme öğrencilerinin bulunduğu sınıfa kolayca uygulanıp etkili sonuçlar alınmıştır. Bu öğrenme ortamı sayesinde e-ticaret ve güvenlik derslerinde öğrencilerin denklemlerin okunması ve yorumlanması sağlanmıştır.

Lee (2016) yaptığı çalışmada, Web 2.0 teknolojileriyle bağlantılı olarak görev temelli öğrenme stratejisinin uygulama olanaklarını araştırmıştır. Bu amaçla görevler ve çevrimiçi araçlar kurs çalışmasına dahil edildi. Kursun sonucunda kullanılan görevlerin ve çevrimiçi araçların farklı şekillerde öğrenenleri desteklediği gözlemlenmiştir. Yapılandırılmış görevler, öğrencilerin içerik oluşturmak için özgün çalışmalarını sağlarken, açık uçlu görevler sayesinde sosyal etkileşim yoluyla belirli bir konunun öğrenilmesinde öğrencilere özgürlük sağladığı tespit edilmiştir. Çevrimiçi ortamın modellemesi ve hızlı geri bildirimi sayesinde öğrencilerin kendi kendini düzenleme çabaları önemli ölçüde etkilemiştir.

Gawlik-Kobylińska (2017) 124 yetişkin öğrencinin katılım gösterdiği çalışmada görev temelli yaklaşımın sanal ortamda gerçekleştirilen görevlerin öğrenci yeterliliklerini artırdığına, onları öğrenme sürecine daha fazla dahil olmalarına ve geleneksel eğitimlerden daha çekici olduğunu algılamalarına yardımcı olduğunu ortaya koymuştur. Sanal ortamda öğrenciler için görevler oluşturmanın güvenlik ve emniyet eğitiminin ilgi çekici olmasını sağladığını belirtmiştir.

González (2017) yaptığı çalışmada, görev temelli dil eğitiminin 1980'lerden itibaren araştırmacıların dikkatini çektiğini ve zengileşmekte olan literatürü göz önünde bulundurarak teknolojinin ve görev temelli dil eğitiminin olgunlaşmasına yardımcı olduğunu öne sürmüştür. Aynı zamanda araştırma, teknoloji ve görev temelli dil öğretiminin karşılıklı katkılarını incelemiş ve çevrimiçi ortamlarda görev temelli dil eğitiminin uygulama ve araştırmadaki zorluklarını özetlemiştir.

Zolotarev vd., (2021) yaptıkları çalışmada, lisans son sınıf ve bilgi güvenliği yüksek lisans son sınıf öğrencileri üzerinde bilgi güvenliği farkındalığını artırmak amacıyla rol ve görev temelli ortam tasarlamışlardır. Araştırma sonunda araştırmacılar tasarlanan ortamın bilgi güvenliği farkındalığı için ortaya koyduğu faydaları, gerçek bir durumun simüle edilmesi, oyuncuların etkileşimindeki psikolojik engellerin kaldırılması, farklı ortamlara entegre edilmesi zor olan pratik vakalara erişim olanağı sağlaması olarak sıralamışlardır..

ÜÇÜNCÜ BÖLÜM
ARAŞTIRMA YÖNTEMİ/MATERYAL VE YÖNTEM

Bu bölümde araştırmanın modeli, çalışma grubu, araştırmada kullanılan deneysel desen, araştırmanın uygulama aşaması, veri toplama teknikleri, veri toplama araçları, çalışmadan elde edilen veriler ve bu verilerin analizinde kullanılan istatistiksel işlemler yer almaktadır.

3.1. Araştırmanın Yöntemi

Araştırmanın modeli, araştırma sorularına cevap vermeyi ya da araştırmanın hipotezlerini test etmeyi sağlayan, verilerin çalışmanın amacına uygun olarak toplanmasını adına gerekli koşulların düzenlenmesini sağlamaktadır (Balcı, 2009). Bu doğrultuda iki ayrı bölümden oluşan araştırmanın ilk bölümünde ortaokul düzeyi bilgi güvenliği farkındalığı ölçeğinin geliştirilmesi çalışması gerçekleştirilmiştir. Bilgi güvenliği farkındalıklarının arttırılmasına yönelik görev temelli çevrimiçi öğrenme ortamının etkisinin belirlenmesi ve geliştirilen öğrenme ortamına ve sürecine yönelik öğrencilerin görüşlerinin belirlenmesinin amaçlandığı araştırmanın ikinci bölümünde ise karma araştırma yöntemlerinden açıklayıcı sıralı desen kullanılmıştır. Araştırma için üzerinde çalışılan alanın etik açıdan uygunluğuna dair Çanakkale Onsekiz Mart Üniversitesi Etik Kurulu'ndan ve anket çalışmasına dair Çanakkale İl Milli Eğitim Müdürlüğü'nden gerekli izinler alınmıştır. Alınan etik kurul onayı ve anket oluru EK5 ve EK6'da sunulmuştur.

Çalışmanın ilk aşaması olan ölçek geliştirme çalışmasında; faktör analizi, geçerlilik oranı ve güvenirlik (iç ve test- tekrar test) katsayıları ile madde analizine dayanan kuramsal ölçek geliştirme modeli kullanılmıştır (Yurdagül, 2005). Ölçek geliştirme ilk önce madde havuzunun hazırlanmasıyla başlayan, ardından geçerlik ve güvenirlik çalışmaları ile devam eden kapsamlı bir çalışmadır. Bir ölçek adına pek çok geçerlik ölçütünden söz edilse de Karasar'a (2005) göre en çok yararlanılanlar: kapsam geçerliği (content validity), uygulama geçerliği (predictive validity) ve yapı geçerliğidir (construct validitiy). Bu araştırmada ölçek geliştirme bölümünün ilk aşamasında geçerlik çalışması, ardından verilerin faktör analizine

uygun olup olmadığı Kaiser-Meyer-Olkin(KMO) testi ve Barlett Küresellik Testi kullanılarak değerlendirilmiştir. Ortaokul Düzeyi Bilgi Güvenliği Farkındalık Ölçeği'nin (OBGFÖ) yapı geçerliğini ölçmek için maksimum değişkenli dik döndürme yöntemi ile Açımlayıcı Faktör Analizi (AFA) yapılmıştır. OBGFÖ'nin alt boyutları ve toplam güvenirlikleri Cronbach Alfa iç tutarlık katsayısı hesaplanmıştır. Ayrıca AFA ile tespit edilen teorik faktör yapısının doğruluğunun test edilebilmesi için Doğrulayıcı Faktör Analizi (DFA) yapılmıştır.

Ölçek geliştirme süreci sonrasında karma yöntemle tasarlanan çalışmanın uygulama aşamasına geçilmiştir. Uygulama aşamasında, karma yöntem sayesinde hem nicel hem de nitel araştırma yöntemlerinin güçlü yönlerinden faydalanabilmekte ve her bir yöntemin sınırlılığının üstesinden gelebilmektedir (Creswell, 2003; Creswell ve Plano Clark, 2007; Johnson ve Christensen, 2008). Green vd., (2005) yaptıkları çalışmada nicel yaklaşımın birçok katılımcıya ulaşmayı sağladığını ve gözlem, görüşme gibi nitel yaklaşımların ise araştırmanın daha derinlemesine analize edilmesine olanak sağladığını öne sürmüştür. Bunun yanında Creswell (2017) karma yöntem yaklaşımını, araştırmacının araştırma problemlerini anlamak için nicel ve nitel verileri topladığı iki veri setini birbiriyle bütünleştirdiğini ardından bu bütünleştirmenin avantajlarının kullandığını bir araştırma yöntemi olarak tanımlamaktadır. Yine Curlette (2006) karma yöntem yaklaşımını desteklemekte ve nitel yaklaşım kullanılarak toplanan verilerin nicel boyutu destekleyeceğini savunmuştur. Bunlara ek olarak karma araştırma yöntemi veri toplama aracı geliştirmeyi veya bir kavrama ait süreçleri ve sonuçları birlikte incelemeyi gerektiren çalışmalara önemli katkılar sunmaktadır (Yıldırım ve Şimşek, 2011). Cresswell (2005), karma araştırma yöntemini üç farklı desen ile açıklamıştır. Bunlar çeşitlemeli karma yöntem deseni (triangulation mixed method design), açıklayıcı karma yöntem deseni (explanatory mixed method design) ve açımlayıcı karma yöntem desenidir (exploratory mixed methods designs). Çeşitlemeli karma yöntem deseninde araştırmanın nicel ve nitel verileri eş zamanlı olarak toplanmaktadır ve toplanan verilerin araştırma içerisindeki ağırlığı birbirine eşittir (Creswell ve Plano-Clark, 2007). Açıklayıcı karma yöntem deseninde ise, öncelikle nicel veriler toplanır ve analiz edilir arından nicel verileri açıklamak ve derinlemesine incelemek amacıyla nitel veriler toplanıp analiz edilmektedir (Creswell, 2005). Üçüncü karma yöntem deseni olan açımlayıcı karma yöntem deseninde ise, öncelikle nitel veriler toplanır ardından

nicel veriler yardımıyla nitel veride bulunan ilişkileri açıklamaktadır (Creswell, 2005). Çalışmanın uygulama aşamasında, karma araştırma yöntemlerinden açıklayıcı sıralı desen benimsenmiş ve araştırma yöntemi tablo 2'de sunulmuştur.

Tablo 2

Açıklayıcı karma yöntem tasarımı

Nicel		**Nitel**
Yarı deneysel çalışma veri ve sonuçları	**Takip eden süreç (Follow-up)**	Açık uçlu soru formu veri ve sonuçları

Açıklayıcı sıralı desenin amacı, araştırma problemine verinin toplanması ve analizi için nicel boyutta başlayıp ardından nicel sonuçları açıklamak için nitel boyutun yürütülmesidir (Creswell, 2005). Bu desen araştırmanın birbiri üzerine inşa edilen kolaylıkla çözümlenebilen ve birbirinden ayırt edilebilen iki aşamadan gücünü almaktadır. Büyüköztürk vd., (2016), açıklayıcı karma yöntem deseninde, bir yöntemin başarısına yönelik öğrenci başarıları analiz edildikten sonra yönteme yönelik öğrenci görüşlerinin ortaya koyulabileceğini belirtmektedir. Bu doğrultuda çalışma nicel ve nitel olmak üzere iki boyuttan oluşmaktadır. Öğrencilerin bilgi güvenliği farkındalığının sağlanmasına yönelik çevrimiçi görev temelli ortamın etkisinin belirlenmesini tespit etmek için çalışmanın nicel boyutunda öntest-sontest kontrol gruplu 2X2'lik bir split plot yarı deneysel desen kullanılmıştır (Büyüköztürk vd., 2016). Yarı deneysel yöntem deney ve kontrol gruplarının rastgele oluşturulamadığı durumlarda, hali hazırda bulunan sınıflar için kullanılabilmektedir (Fraenkel ve Wallen, 2011). Bu bağlamda araştırma deseninin görünümü tablo 3'te sunulmuştur.

Tablo 3

Öntest-sontest kontrol gruplu 2X2’lik split plot desen modeli

Grup	**Deney Öncesi**	**Deneysel İşlem**	**Deney Sonrası**
Deney	Öntest(OBGFÖ)	Görev Temelli Çevrimiçi Öğrenme Yöntemi	Sontest(OBGFÖ)
Kontrol	Öntest(OBGFÖ)	Geleneksel Ortam	Sontest(OBGFÖ)

OBGFÖ: Ortaokul Düzeyi Bilgi Güvenliği Farkındalık Ölçeği
Bağımsız değişken: Görev Temelli Çevrimiçi Öğrenme Ortamı
Bağımlı Değişken: Öğrencilerin bilgi güvenliği farkındalık düzeyleri

Uygulama aşamasının nitel boyutunda ise öğrencilerin görev temelli çevrimiçi öğrenme ortamına ve sürecine ilişkin görüşleri açık uçlu soru formu kullanılarak toplanmıştır. Açık uçlu sorular katılımcılardan özgür bir şekilde cevap vermeleri istendiğinde tercih edilir ve en büyük avantajı araştırmacının beklemediği cevaplar almasından dolayı konu hakkında daha ayrıntılı ve geniş bilgiye sahip olunmasıdır (Büyüköztürk, 2005). Çalışmada nicel ve nitel verilerin bütünleştirilmesi sayesinde bulguların geçerliliği ve güvenirliğinin arttırıldığı düşünülmektedir.

3.2. Araştırmanın Çalışma Grubu

Ölçek geliştirme ve uygulama süreci olmak üzere iki boyuttan oluşan çalışmanın ölçek geliştirme sürecinin çalışma grubunu 2021-2022 eğitim öğretim yılında ortaokul düzeyinde 11 farklı okulda öğrenim görmekte olan 702 öğrenci oluşturmaktadır. Ancak toplanan veriler üzerinde çalışma gerçekleştirilmiş olup ve 675 tanesinin istatiksel analize uygun olduğu tespit edilmiştir. Ölçme aracının geliştirilmesi sürecinin Açımlayıcı Faktör Analizi (AFA) aşamasında 410 öğrencinin verisi değerlendirilmiş ve analizler sonucunda ölçme aracı yeniden düzenlenmiştir. Elde edilen yeni form ise çalışmanın Doğrulayıcı Faktör Analizi (DFA) için tekrar uygulanmış ve bu aşamada toplam 265 öğrenciden elde edilen verilerin analizi gerçekleştirilmiştir. Ölçek geliştirme aşamasında çalışmaya katılan öğrencilerin cinsiyete ve sınıf düzeyine göre dağılımı tablo 4’te verilmiştir.

Tablo 4

Öğrencilerin sınıf düzeyi ve cinsiyet dağılımları (birinci aşama)

		AFA Aşaması		DFA Aşaması		Toplam	
		f	**%**	**f**	**%**	**f**	**%**
Cinsiyet	Kız	210	51.21	145	54,71	355	52,60
	Erkek	200	48,79	120	45,29	320	47,40
	Toplam	**410**	**100**	**265**	**100**	**675**	**100**
Sınıf Düzeyi	5. Sınıf	110	26,82	66	24,90	176	26,07
	6. Sınıf	86	20,98	72	27,16	158	23,40
	7. Sınıf	108	26,35	60	22,64	168	24,88
	8. Sınıf	106	25,85	67	25,28	173	25,62
	Toplam	**410**	**100**	**265**	**100**	**675**	**100**

Araştırmanın AFA ve DFA süreçlerinde verileri analiz edilen 675 öğrencinin cinsiyetlerine göre dağılımı incelendiğinde 355'i (%52,60) kız, 320'si (%47,40) ise erkek öğrencilerden oluşmaktadır. Öğrencilerin 176'sı (%26,07) 5. Sınıf, 158'i (%23,4) 6. Sınıf, 168'i (%24,88) 7. Sınıf ve 173'ü (%25,62) 8. Sınıfta öğrenimlerine devam ettiği görülmüştür.

Ölçek geliştirme sürecinin sonrasında uygulama aşamasının çalışma grubunu, 2021-2022 eğitim öğretim yılı bahar döneminde ortaokul 6.sınıfta öğrenim gören ve 20'si deney grubu, 20'si kontrol grubu olmak üzere toplam 40 öğrenci oluşturmaktadır. Çalışma grubu seçiminde; deneysel işlemlerin sürekliliğini sağlama, deneklere ulaşabilme kolaylığı ve öğrencilerin konuya yönelik ön bilgi düzeylerinin birbirine yakın olması kıstasları dikkate alınmıştır. Uygulama öncesi belirlenen iki grubun ön bilgilerinin belirlenmesi ve dağılımın homejenliğini test etmek amacıyla öğrencilere öntest uygulanmıştır. Uygulanan öntest sonucunda, uygulamanın gerçekleştirildiği sınıflar arasında homejenliğin sağlandığı (Levene Statistic F=0,833, p>.05) tespit edilmiştir. Deney ve kontrol grubu öğrencilerinin yarı deneysel işlem öncesinde bilgi güvenliği farkındalık düzeyi öntest puanları arasında istatiksel olarak anlamlı bir farklılık olup olmadığına ilişkin bağımsız gruplar t testi yapılmıştır. Yapılan analiz sonucunda, öğrencilerinin öntest bilgi güvenliği farkındalık düzeyi puanları arasında anlamlı bir farklılığın olmadığı görülmektedir (t=1,658; p>,05). Elde edilen bu sonuçlar doğrultusunda, iki ayrı şubenin deney ve kontrol grubu olarak iki farklı grupta değerlendirilmesine karar verilmiştir. Toplam 5 hafta sürecek olan uygulama

sürecinde dersler deney grubunda yer alan öğrencilere geleneksel öğrenme süreçlerinin yanı sıra araştırmacı tarafından hazırlanmış olan görev temelli çevrimiçi ortam sunulmuştur. Kontrol grubunda bulunan öğrencilere ise herhangi bir müdahale yapılmamış ve geleneksel öğrenme süreçlerinde almış oldukları eğitimlerine devam etmişlerdir.

Tablo 5

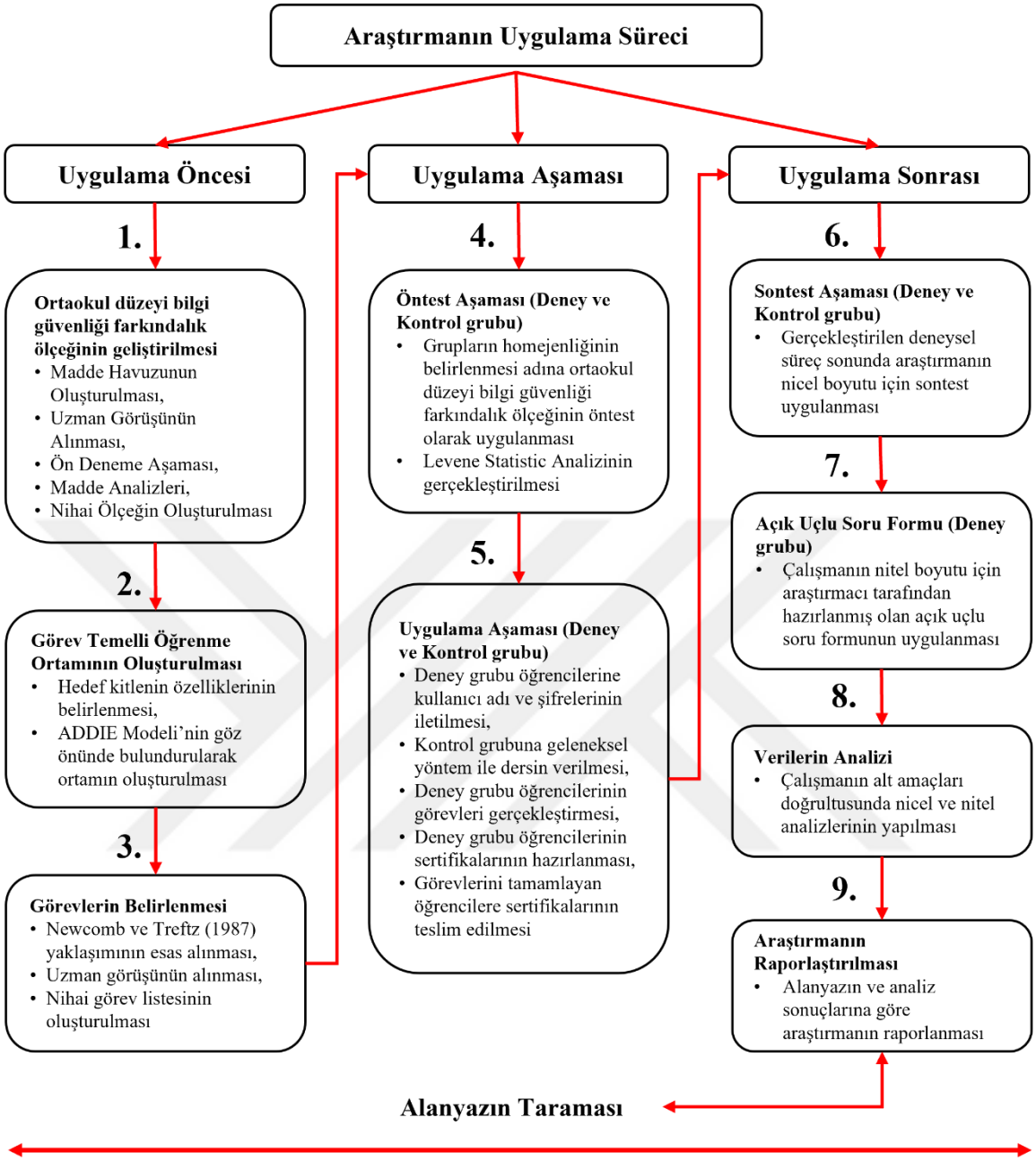
Deney ve kontrol grubunu oluşturan öğrencilerin cinsiyete göre dağılımları (ikinci aşama)

	Deney Grubu		**Kontrol Grubu**		**Toplam**	
Cinsiyet	N	%	N	%	**N**	**%**
Kız	8	%40	9	%45	**17**	**%42,5**
Erkek	12	%60	11	%55	**23**	**%57,5**
Toplam	**20**	**%100**	**20**	**%100**	**40**	**%100**

Tablo 5'te görüldüğü gibi, deney grubundaki öğrencilerin %40'ı (8 kişi) kız, %60'ı (12 kişi) erkek; kontrol grubundaki öğrencilerin %45'i (9 kişi) kız, %55'i (11 kişi) erkek öğrencilerden oluşmaktadır. Çalışmada deney ve kontrol grubu olmak üzere toplam 40 öğrenci yer almıştır. Çalışmaya katılan 40 öğrencinin %42,5'i (17 kişi) kız, %57,5'i (23 kişi) erkektir. Nitel çalışma ise çalışmanın deney grubunu oluşturan 20 öğrenci ile yarı deneysel süreç sonrasında gerçekleştirilmiştir.

3.3. Uygulama Aşaması

Araştırmanın uygulama aşaması öncesi öğrencilerin bilgi güvenliği farkındalık düzeylerinin belirlenmesine yönelik ortaokul düzeyinde uygun ölçek bulunamamış ve öncelikle ölçek geliştirme çalışması gerçekleştirilmiştir. İkinci aşamada ise görev temelli çevrimiçi ortamının oluşturulması ve öğrencilerin uygulama süresince gerçekleştireceği görevler hazırlanması süreci gerçekleştirilmiştir. Çalışmanın uygulama sürecinde Şekil 2'de gösterilen aşamalar izlenmiştir.

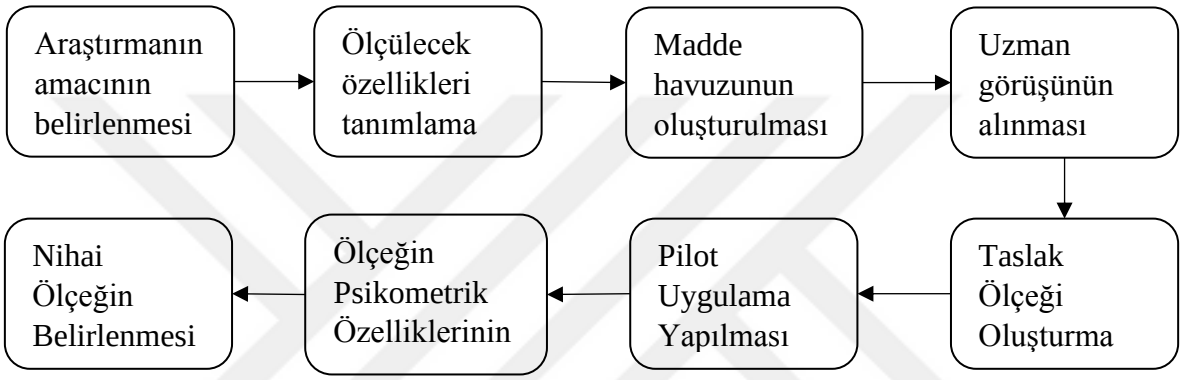


Şekil 2. Çalışmanın uygulama aşamasında izlenen süreç

3.3.1. Ortaokul Düzeyi Bilgi Güvenliği Farkındalığı Ölçeği Geliştirme Çalışması

Ölçek kavramı matematiksel niteliklerin dışında eğitim ve psikoloji gibi davranış bilimlerinin alanında, konu ve içerik ile ilgili veri toplamak amacıyla kullanılır (Torgerson, 1958). Araştırmacılar (Pasquali, 2010; Clark ve Watson, 2019; Devellis, 2021) ölçek

geliştirme çalışmalarının karmaşık ve sistemli prosedürleri içerdiğini belirtmektedir. Çoğunlukla ölçek geliştirme çalışmaları, deneysel süreç veya kavramsal süreçlerden oluşmaktadır. (Yurdagül, 2005). Ölçek geliştirme çalışmasının deneysel sürecinde literatür taraması ya da uzman değerlendirme yaklaşımları sayesinde bu çalışmayı gerçekleştirebilmek adına DeVellis'in (2014), Tezbaşaran'ın (2008), ve Karasar'ın (2005) ölçek geliştirme aşamaları göz önünde bulundurularak 5'li likert tipi bir ölçek geliştirilmiştir. Araştırmada uygulanan ölçek geliştirme işlem basamakları şekil 3'te sunulmuştur.



Şekil 3. Ölçek geliştirme basamakları (DeVellis, 2014; Karasar, 2005; Tezbaşaran, 2008)

Şekil 3'te görüldüğü gibi likert tipi ölçekler hazırlanırken göz önünde bulundurulması gereken basamaklar bulunmaktadır. Araştırmanın ölçek geliştirme aşamasında ise izlenen yol Tablo 6'da sunulmuştur.

Tablo 6

Ortaokul düzeyi bilgi güvenliği farkındalık ölçeği geliştirme süreci

Ölçek Geliştirme Adımları		Açıklamalar
1. Adım Yapıyı Belirleme	Ölçeğin Amacını Belirleme	Ortaokul kademesinde öğrenim gören öğrencilerin, bilgi güvenliği farkındalık düzeylerini ortaya çıkaracak bir ölçek çalışması amaçlanmıştır.
	Alanyazın Taraması	Alanyazında "Bilgi Güvenliği", "Bilgi Güvenliği Farkındalığı", "Siber Saldırılar" ile ilgili araştırmalar incelenmiştir.
	Ölçülecek Niteliklerin Tanımlanması	Alanyazın taramasının ardından hangi boyutların ve alt boyutların ele alınması ve çalışma için en temel özelliklerin neler olması gerektiğine dair kararlar verilmiştir.
	Maddelerin Formatına Karar Verme	Ölçekte yer alacak maddeler "bilirim/bilmem, yaparım, yapmam" şeklinde hazırlanmıştır.
2.Adım Madde Havuzu	Madde Havuzunun Oluşturulması	Yapı belirleme ve görüşülen ilk çalışma grubu sonrası, alanyazından da faydalanılarak 124 maddelik madde havuzu oluşturulmuştur.
	Maddelere Yönelik Dereceli Puanlama Cetveli Oluşturulması	Ölçek maddeleri için 5'li likert tipi ölçek derecelendirilmesi uygun görülmüştür. Uzman görüşü için 3'lü likert derecelendirme yapılmıştır.
3.Adım Uzman Görüşü Alma	Maddeler Hakkında Uzman Görüşü Alma	Bilgisayar ve Öğretim Teknolojileri Uzmanı toplam 9 Uzman, her madde için 3'lü likert derecelendirme yaparak görüşleri alınmıştır.
	Maddelerin Gözden Geçirilmesi/Gerekli Düzeltmelerin Yapılması	Uzmanlardan gelen görüşlere göre maddeler gözden geçirilerek gerekli görülen düzeltmeler yapılmıştır.
	Kapsam ve Görünüm Geçerlik Çalışması	Uzman görüşleri Lawshe tekniğinden yararlanılarak 20 madde çıkarılmış ve kapsam geçerlilik değerleri hazırlanmıştır.
4.Adım Pilot Çalışması	Pilot Uygulama	Pilot uygulama ortaokul kademesinde öğrenim gören 410 öğrenci üzerinde AFA ve 265 öğrenci üzerinde DFA olarak toplam 675 öğrenci üzerinde uygulanmıştır.
5.Adım Madde Analizi	Madde Analizleri	Pilot uygulayıcılar 5'li likert tipine göre derecelendirme ile ölçek üzerinde değerlendirme yapmıştır. Ölçeğin geçerlik ve faktör analizi, Açımlayıcı Faktör Analizi (AFA) ve Doğrulayıcı Faktör Analizi (DFA) yaklaşımları göz önünde bulundurularak yapılmıştır. Ölçeğin güvenirliği için Cronbach Alfa iç tutarlılık katsayısına bakılmıştır.
6.Adım Nihai Ölçeğin Belirlenmesi	İstatiksel Analiz	Katılımcılara dair istatiksel analizler yapılarak her madde için geçerlik – güvenirlik analizleri yapılara ölçeğe son hali verilmiştir.

Araştırmanın yapısı için ilk olarak ölçeğin amacının belirlenmesi sırasında literatür taraması yapılarak maddeler oluşturulmuştur. Bununla birlikte Millî Eğitim Bakanlığına

bağlı okulların ortaokul kademesinde öğrenim gören öğrencilerin özellikleri düşünüldüğünde bilgi güvenliği farkındalığını ortaya çıkaracak alanyazında çalışma bulunmaması sebebiyle özgün bir ölçek çalışması olduğu görülmektedir. Bu doğrultuda aşağıda yer alan başlıklar altında detaylandırılan ölçek geliştirme adımları izlenmiştir.

Madde Havuzu Aşaması: Ölçek geliştirmenin en önemli adımlarından biri olan literatür aşamasında alanyazın incelenerek, yerli ve yabancı alanyazında bilgi, bilgi güvenliği, bilgi güvenliği farkındalığı ve siber tehditler ile ilgili araştırmalar incelenmiş ve ölçekte kullanılacak ifadeler belirlenmiştir. Literatür araştırmasının ardından araştırma için öncelikli olarak hangi temel özelliklere yer verileceğine karar verilmiştir. Belirlenen niteliklere özgü maddeler kullanılarak ölçeğin yapısı oluşturulmuştur. Bu bağlamda "Çevrimiçi Güvenlik farkındalığı", "Siber Tehditler Farkındalığı" ve "Çevrimiçi Merak" alt boyutları oluşturulmuştur. Bilgi güvenliği farkındalığına yönelik kategori ve madde sayıları tablo 7'de sunulmuştur.

Tablo 7

Bilgi güvenliği farkındalığına ilişkin kategori ve madde sayıları

Kategoriler	**Nitelikler**	**Madde Sayısı**
Güvenlik	Bilgi güvenliği, Bilgi güvenliği farkındalığı, Şifre güvenliği, verilerin güvende tutulması	24
Siber Tehditler	Virüs ve casus yazılımlar, Hizmet aksattırma saldırıları, Oltalama, Korsan yazılımlar, Sosyal mühendislik, Kimlik hırsızlığı	33
Bilişim Teknolojileri	Cep telefonları, kullanım süresi, kişisel bilgiler, taşınabilir cihazlar, Kablosuz ağ güvenliği, Yazılımlar, taşınabilir cihazlar, anlık mesajlaşma, e-posta, web sitesi sertifikaları, işletim sistemleri	34
Mahremiyet	Telif hakkı ihlalleri, Tarayıcılara ait güvenlik işlemleri, Çevrimiçi güvenli alışveriş, kişisel bilgilerin korunması	18
Siber Zorbalık	Siber zorbalık, Bilişim suçları, Dolandırıcılık, Sosyal medya, Sosyal medya güvenliği	15
Toplam		**124**

Ölçekte yer alması düşünülen maddeler farkındalık kavramı üzerinde durularak "bilirim/bilmem, ederim/etmem" şeklinde cümle yapısı ile oluşturulmuştur. Öğrencilerin ölçekte bulunan maddelere katılma düzeylerini belirlemek üzere "kesinlikle katılmıyorum

(1)", "katılmıyorum (2)", "kararsızım" (3)", "katılıyorum (4)" ve "kesinlikle katılıyorum (5)" formatında likert tipi beşli derecelendirme ölçeği kullanılmıştır. Alanyazın taraması ve nitelik tanımlaması işlemi ardından 5 kategoride toplam 124 maddelik "OBGFÖ" ölçeği madde havuzu oluşturulmuştur.

Kapsam Geçerlilik Aşaması: Ölçülmesi hedeflenen nitelik ile ölçek maddeleri arasındaki bağıntı, ölçeğin geçerliği ile alakalıdır. Ölçekte bulunan maddenin ölçülmesi amaçlanan özelliği kapsama (kapsam geçerliği) ya da maddenin ilgili yapıyı yorma (yapı geçerliği) gücünü belirlemek amacıyla çalışmalara ihtiyaç vardır (McGartland vd., 2003). Önsel çalışmalar ile ortaya çıkan uzman görüşleri arasındaki uyum aynı zamanda kapsam geçerliği ya da yapı geçerliği için birer karar niteliğinde kullanılmaktadır. Lawshe (1975) tarafından geliştirilmiş olan Lawshe tekniği olarak bilinen yaklaşım ile kapsam geçerlik değerlerinin belirlenmesi işlemi aşağıdaki adımlardan oluşmaktadır.

- Konu uzmanları ekibinin oluşturulması
- Uzman görüşü formlarının hazırlanması
- Uzman görüşlerinin elde edilmesi
- Maddelere yönelik kapsam geçerlik oranlarının (KGO= CVR=Content Validity Ratio) elde edilmesi
- Kapsam geçerlik indekslerinin (KGI=CVI= Content Validity Index) elde edilmesi
- Kapsam geçerlik değerleri ölçütlerine göre nihai ölçeğin oluşturulması

Kapsam geçerliliğin hesaplanması için yapılacak olan değerlendirmede objektif sonuçlar ortaya çıkabilmesi adına uzman ekibinin niteliği ve büyüklüğü (5-40) büyük önem arz etmektedir (Lawshe, 1975; Veneziano ve Hooper, 1997). Her bir maddeye yönelik uzman görüşleri, "uygun değildir", "düzeltilmeli", "uygun" şeklinde üçlü derecelendirilmektedir. Kapsam geçerliliğin dışında maddenin anlaşılabilirliği, hedef kitleye uygunluğu vb. amacıyla da uzman görüşü derecelendirilebilir (Lawshe, 1975). Ayrıca uzmanlar tarafından "cevabınız düzeltilmeli ise ne şekilde olması gerektiği ile ilgili önerisini" açıklamalar bölümüne görüşlerini yazmaları istenmiştir. Bu bağlamda uzmanlara gönderilen uzman görüş formundan sonra uzmanların maddelere ait görüşleri hesaplanarak kapsam geçerlilik oranları (KGO) elde edilir. KGO, bir maddeye ilişkin "Uygun" görüşünü

belirten uzman sayısının, toplam uzman sayısının yarısına oranının 1 eksiği ile elde edilir (Wilson vd., 2012).

$$\text{KGO} = \frac{\text{Nu}}{\text{N/2}} - 1 \qquad (3.1)$$

Denklem 3.1'e göre Nu, maddeye "uygun" diyen uzmanların sayısını, N ise toplam uzman sayısını göstermektedir. Denklem 3.1'e göre; uzmanların yarısı maddeye yönelik "uygun" şeklinde görüş verdiklerinde KGO=0, yarısından fazlası "uygun" şeklinde görüş vermiş ise KGO>0, yarısından azı "uygun" şeklinde görüş vermiş ise KGO<0 olacaktır. KGO değerleri negatif (sıfırdan küçük) ya da 0 (sıfır) ise maddenin kapsam geçerliliği yoktur. Dolayısıyla ölçekte bulunan bu maddeler doğrudan çıkarılır (Lawshe, 1975; Wilson vd., 2012). Ortaya çıkan KGO değerlerinin istatistiksel olarak anlamlılığı test etmek amacıyla kapsam geçerlilik ölçütlerine ilişkin Veneziano ve Hooper, 1997'de uzman sayısına göre a=,05 anlamlılık düzeyinde KGO'ların minimum değerleri için, farklı istatiksel analizler tabloya dönüştürmüşlerdir.

Tablo 8

a= ,05 anlamlılık düzeyinde kgo'ların minimum değerleri

Uzman Sayısı	Minimum Değer	Uzman Sayısı	Minimum Değer
5	,99	12	,56
6	,99	13	,54
7	,99	14	,51
8	,78	15	,49
9	,75	20	,42
10	,62	25	,37
11	,59	40+	,29

Madde havuzu oluşturulduktan sonra ortaya çıkan 124 maddelik ilk deneme formu, Bilgisayar ve Öğretim Teknolojileri Eğitimi alanından 4, Ölçme Değerlendirme alanından 1 ve çeşitli okullarda görevli olan 4 Bilişim Teknolojileri öğretmeni olmak üzere 9 uzman görüşü alınmıştır. Uzmanlar her bir maddeyi, bilgi güvenliğine yönelik farkındalığı ölçebilme, ilgili kategoriyle ilişkili olma, ifadenin uygunluğu ve anlaşılırlığı başlıkları altından değerlendirmişlerdir.

Tablo 9

Ölçek kategorileri ve kapsam geçerlilik oranları

Kategoriler	Başlangıç Madde Sayısı	Başlangıç KGO	Madde Sayısı	KGO
Bilgi Güvenliği	24	,58	19	,84
Siber Tehditler ve Siber Güvenlik	33	,74	27	,86
Çevrimiçi Teknolojiler	34	,78	28	,92
Mahremiyet	18	,86	16	,94
Siber Zorbalık ve Siber Mağdur	15	,88	14	,96
Toplam	**124**	**,77**	**104**	

Uzman Sayısı	**9**
Kapsam Geçerlik Ölçütü	**,75**
Kapsam Geçerlik İndeksi	**,90**

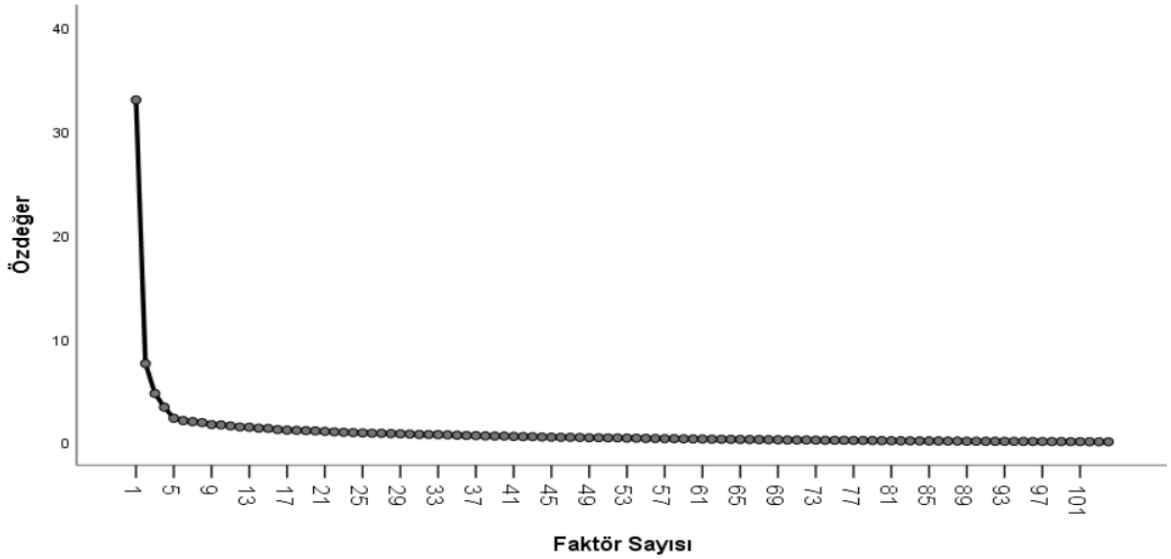
Alanında 9 uzmanın maddelere ilişkin belirttikleri görüşler üzerinden Lawshe tekniği ile kapsam geçerlik oranları hesaplanmıştır. Gerçekleştirilen ilk uygulama sonucunda elde edilen veriler doğrultusunda ortaya çıkan Kapsam Geçerlilik Oranı (KGO) değeri, Veneziano ve Hooper (1997) tarafından tabloya dönüştürülen kapsam geçerlik ölçütü (KGO9=,75) ile karşılaştırma yapılmıştır. İstatistiksel olarak α=,05 anlamlılık düzeyinde gerçekleştirilen analizler sonucunda belirtilen değerin altında değer alan 20 madde çalışma kapsamından çıkartılmış ve üzerinde düzeltmeler yapılan maddelerle birlikte çalışma sonucunda oluşan 104 maddelik formun kapsam geçerlik indeksi ,90 olarak hesaplanmıştır.

Ön Deneme Aşaması: Oluşturulan ölçek toplamda 6 ay süren veri toplama süreci sonrasında ilköğretim düzeyi ortaokul kademesinde eğitim görmekte olan 702 öğrenci ölçeği doldurmuştur. Analiz öncesi eksik ve hatalı veriler incelenmiş ve ölçeği dolduran 702 öğrenciden 675 öğrencinin verisinin istatiksel analize uygun olduğu tespit edilmiştir. Ölçme aracının geliştirilmesi sürecinin AFA aşamasında 410 öğrencinin verisi değerlendirilmiş ve analizler sonucunda ölçme aracı yeniden düzenlenmiştir. Elde edilen yeni form ise çalışmanın DFA için tekrar uygulanmış ve bu aşamada toplam 265 öğrenciden elde edilen veriler ile ölçeğin geçerlik ve güvenirlik çalışmaları yapılmıştır.

Faktör Analizi Aşaması: Çalışmanın örneklem büyüklüğünün belirlenmesinde madde ve faktör sayısı gibi bağıl ölçütler göz önünde bulundurulmuştur. Bu noktada genel olarak örneklem büyüklüğüne yönelik; ölçme aracını oluşturan toplam madde sayısının 5-10 katı olması (Kass ve Tinsley, 1979; Kline, 1994) ve en az 300 örneklem sayısının faktör analizi için uygun olabileceği genel kuralı ortaya konulmaktadır (Çokluk vd., 2010). Kline (1994) ise büyük örneklemler üzerinde çalışmanın daha uygun olacağını vurgulamakla birlikte mutlak ölçüt olarak 200 kişilik örneklemin yeterli olabileceğini belirtmiştir. Diğer taraftan genel olarak ölçek geliştirme süreçlerinde ideal olanın; AFA ve DFA'nın farklı örneklem gruplarından elde edilen verilerin üzerinde yapılması olduğu ifade edilmektedir (Çakmak vd., 2014). Bu doğrultuda gerçekleştirilen çalışmanın örneklemini oluşturan ilk uygulama grubu üzerinde AFA (n1=410), ikinci uygulama grubu üzerinde ise DFA (n2=265) yapılmıştır. Araştırmada elde edilen verilerin AFA için uygunluğunun saptanması amacıyla; Kaiser-Meyer-Olkin (KMO) ile birlikte Barlett Küresellik testi ölçümlerinden faydalanılmıştır. Çokluk vd., (2010) örneklem büyüklüğüne göre ortaya çıkan değerin .50'den düşük olması durumunda teste devam edilmemesi gerektiğini ancak .90'ın üzerinde bir değer alması durumunda ise "mükemmel" olarak nitelendirmiştir. Gerçekleştirilen araştırmada KMO katsayı değeri ,903 olarak belirlenmiştir. Elde edilen bu sonuç doğrultusunda faktör analizinin yapabilmesi için veri yapısının mükemmel düzeyde yeterli olduğu yönünde değerlendirme yapılabilir. Ayrıca yapılan analizler Barlett Küresellik testinin ,01 düzeyinde anlamlı olduğunu göstermiştir [$\chi 2$= 34349,808; df=5356; p=,000]. Elde edilen bu bulgular çalışmanın örnekleminin yeterli seviyede olduğu, verilerin çok değişkenli normal dağılımdan geldiği ve dolayısıyla da faktör analizi için bir diğer varsayımın karşılandığı anlamına gelmektedir.

Ölçme aracının faktör yapısının belirlenmesi amacıyla öncelikle döndürülmemiş temel bileşenler analizi yapılmıştır (Tabachnick ve Gidell, 2013). Faktör sayısının belirlenmesi sürecinde Kaiser-Guttman ilkesi gereği özdeğerleri 1 ve üzeri faktörlerin incelenmesi yoluna gidilerek, faktör özdeğerlerine ait çizgi grafiği ile birlikte açıkladıkları varyans oranlarına bakılmıştır (Zwick ve Velicer, 1986). Ölçme aracı özdeğerleri 1 ve üzeri 22 faktör yapısına sahip olduğu ve faktörlerin özdeğeri ile açıklanan toplam varyansa katkı düzeyleri sırasıyla; 1.faktör: 33,03 (%31,76), 2.faktör: 7,59 (%7,29), 3.faktör 4,69 (%4,51), 4.faktör: 3,37 (%3,25), 5.faktör: 2,31 (%2,22), 6.faktör: 2,08 (%2,00), 7.faktör: 1,98

(%1,90), 8.faktör: 1,89; (%1,81), 9.faktör: 1,70 (%1,63), 10.faktör: 1,67 (%1,61), 11.faktör 1,57 (%1,50), 12.faktör: 1,46 (%1,41), 13.faktör: 1,44 (%1,38), 14.faktör: 1,35 (%1,30), 15.faktör: 1,33 (%1,28), 16.faktör: 1,21 (%1,16), 17.faktör: 1,16 (%1,12), 18.faktör: 1,14 (%1,09), 19.faktör: 1,11 (%1,07), 20.faktör: 1,08 (%1,04), 21.faktör: 1,04 (%1,00), 22.faktör: 1,00 (%,96) şeklindedir.



Şekil 4**.** Ölçeğin faktör özdeğerlerine ilişkin çizgi grafiği

Ölçek faktör yapılarının karar sürecinde ortaya konulan çözümlemenin kuramsal olarak temellendirilmesi gerekmektedir (Zwick ve Velicer, 1986). Genel olarak tek faktörlü ölçek yapılarında açıklanan varyans oranının %30 ve üzeri olması yeterli görülürken çok faktörlü yapılarda bu oranının daha fazla olması beklenmektedir (Tabachnick ve Fidell 1996). Açıklanan toplam varyansı yükseltmek için ise faktör sayısını arttırmak ya da faktör yük değeri yüksek olan maddelerin seçilmesi olmak üzere iki yol izlenebilir (Büyüköztürk, 2002). Madde faktör yük değerinin düşük olarak ortaya çıkması o maddenin faktörle yeterli seviyede bir bağlantısının olmadığını göstermektedir. Faktör yük değerlerinin faktör sayısının belirlenmesinde belirleyici rol oynaması için bütüncül ve yüksek bir yapıya sahip olması beklenmektedir (Büyüköztürk, 2002). Faktörde bulunan maddelerin ,60 ve üzeri yük değerleri yüksek seviye, ,30 ile ,59 arası yük değerleri ise orta seviye büyüklük olarak tanımlanmaktadır (Büyüköztürk, 2002; Watkins, 2021). Bu doğrultudan yola çıkarak ölçek maddelerinin faktörlerle olan ilişkisinin yüksek düzeyde olması, bu maddelerin bir kavramı daha iyi ölçtüğü anlamına geldiği göz önünde bulundurularak çalışmanın özdeğeri 2 ve

faktör yük değeri ,65 olarak belirlenerek analize devam edilmiştir. AFA' ya göre ölçek özdeğeri 2'den büyük olan 6 faktörde toplandığı ve bu faktörlerin açıkladığı varyans değeri ise %51,06 olarak ortaya çıkmıştır. Çokluk vd., (2010) maddenin yük değerinin ,40'tan büyük olması ve madde çıkarılması işlemine binişik maddelerden başlanılması gerektiğini savunmaktadır. Bu çalışmada faktör yük değeri düşük olan maddelerle birlikte binişik maddeler de ölçekten çıkartılmıştır. Bu aşamada açımlayıcı faktör analizi 28 kez tekrarlanmış ve ortaya çıkan maddelerin faktör yük değerleriyle birlikte ortak faktör varyans değerleri Tablo 10'da sunulmuştur.

Tablo 10

Ölçeğin faktör analizi sonuçları

AB*	**M***	**F1**	**OFV***	**AB**	**M**	**F2**	**OFV**	**AB**	**M**	**F3**	**OFV**
Çevrimiçi Güvenlik Farkındalığı	S51	,65	,61	**Çevrimiçi Merak**	S44	,65	,86	**Siber Tehdit Farkındalığı**	S89	,75	,85
	S53	,73	,69		S46	,65	,85		S90	,72	,83
	S54	,68	,54		S78	,67	,55		S92	,71	,76
	S55	,72	,65		S85	,76	,78		S93	,73	,86
	S56	,77	,63		S86	,84	,77		S97	,71	,69
	S57	,75	,57		S91	,74	,72		S99	,74	,83
	S58	,71	,72		S101	,73	,65				
	S59	,75	,64		S103	,77	,85				
	S60	,71	,63		S104	,70	,84				
	S64	,74	,66								
	S65	,69	,71								
	S67	,68	,75								
	S69	,67	,61								
	S70	,66	,80								
	S73	,67	,64								
Özdeğer: 9,91				**Özdeğer:** 4,69				**Özdeğer:** 2,23			
Açıklanan Varyans: 33,04				**Açıklanan Varyans:**15,63				**Açıklanan Varyans:**7,63			
								Açıklanan Toplam Varyans:56,30			
***AB: Alt Boyut, *M: Madde, *OFV: Ortak Faktör Varyansı**											

Tablo 10'da yer alan veriler incelendiğinde 15 maddenin yer aldığı birinci faktöre ilişkin yük değerlerinin ,65 ile ,77 arasında değişim gösterdiği ve maddelere ait ortak faktör varyans değerlerinin ,54 ile ,80 arasında değişim gösterdiği görülmüştür. Birinci faktör

açıklayabildiği toplam varyans %33,04 değerinde olup alanyazın da göz önünde bulundurularak "çevrimiçi güvenlik farkındalığı" olarak isimlendirilmiştir. İkinci faktör 9 maddeden oluşmakta olup maddelere ait faktör yük değerleri ,65 ile ,84, maddelere ait ortak faktör varyans değerleri ise ,55 ile ,86 arasında değişim göstermiştir. İkinci faktörün açıklayabildiği toplam varyans %15,63 değerinde olup alanyazın da göz önünde bulundurularak "çevrimiçi merak" olarak isimlendirilmiştir. Üçüncü faktör ise 6 maddeden oluşmakta olup maddelerin faktör yük değerleri ,71 ile ,75 aralığında, maddelere ait ortak faktör varyans değerleri ise ,69 ile ,86 aralığında değişim göstermektedir. Üçüncü faktörün ise açıklayabildiği toplam varyans %7,63 değerinde olup alanyazın da göz önünde bulundurularak "siber tehdit farkındalığı" olarak isimlendirilmiştir. 30 maddeden oluşan ölçeğin toplam varyansına en düşük desteği ,68 faktör yük değeri ve ,54 ortak faktör varyansı ile 54. Maddenin, en yüksek desteği ise ,73 faktör yük değeri ve ,86 ortak faktör varyansı ile 93. Maddenin verdiği gözlemlenmiştir. Nihai olarak ortaya çıkan 3 faktörlü yapının toplam varyansın %56,30'unu açıkladığı belirlenmiştir. Tavşancıl'a (2005) göre sosyal bilimlerde ölçekte bulunan maddelerin açıklanan varyans oranının %40 ile %60 arasında bir oranda olmasını beklenmektedir. Bu ölçüt doğrultusunda elde edilen 3 faktörlü yapının, ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyini belirlemek için yeterli olduğu söylenebilir. Diğer taraftan ölçeği oluşturan 30 maddenin tamamının faktör yük değeri ,65'in üzerinde kaldığı görülmektedir. Alanyazında ,60 ve üstü yük değeri, yüksek büyüklük olarak tanımlanmakta ve ölçme aracında kesinlikle yer alması beklenen maddeler olarak nitelendirilmektedir (Büyüköztürk, 2006; Kline, 2000; Watkins, 2021). Bu ölçütler doğrultusunda ölçeğin, 3 faktörlü yapı altında toplanan 30 maddenin tamamının yer alması uygun görülmüştür.

Madde Analizleri: Geliştirilen ölçekte bulunan maddelerin, ölçülmek istenen özelliği ölçüp ölçmediği ve ayırt ediciliğini belirlemek amacıyla öncelikle madde-toplam korelasyonları ardından ise üst ve alt %27'lik gruplara ait madde puanları arasında anlamlı bir farkın olup olmadığı t-testi ile analiz edilmiştir. Ölçeğin iç tutarlılığının belirlenmesi amacıyla ise Cronbach Alfa iç tutarlılık katsayısına bakılmıştır. Bu doğrultuda ölçekte yer alan her bir maddenin madde-toplam korelasyonları ile toplam puanlara göre belirlenen üst ve alt %27'lik gruplara ait madde puanları arasındaki farkın anlamlılığının irdelendiği bağımsız t-testi analiz sonuçları Tablo 11'de sunulmuştur.

Tablo 11

Madde analizi sonuçları

F1	Madde	DM-TK*	Ü/A %27*	F2	Madde	DM-TK	Ü/A %27	F3	Madde	DM-TK	Ü/A %27
Çevrimiçi Güvenlik Farkındalığı	S51	,651	10,51	Çevrimiçi Merak	S44	,567	3,334	Siber Tehdit Farkındalığı	S89	,669	9,819
	S53	,658	9,717		S46	,580	2,549		S90	,641	10,03
	S54	,677	12,86		S78	,597	3892		S92	,665	9,332
	S55	,683	12,09		S85	,670	7,078		S93	,681	10,05
	S56	,736	13,42		S86	,775	9,994		S97	,713	12,35
	S57	,676	11,47		S91	,646	7,912		S99	,660	8,737
	S58	,728	17,15		S101	,638	7,893				
	S59	,728	12,27		S103	,691	9,570				
	S60	,705	14,81		S104	,599	10,02				
	S64	,713	13,43								
	S65	,660	12,47								
	S67	,668	11,94								
	S69	,684	14,04								
	S70	,689	14,00								
	S73	,672	13,29								

* DM-TK: Düzeltilmiş Madde-Toplam Korelasyonu

* Ü/A %27: Üst ve Alt %27 Farkın Anlamlılık Testi (Bağımsız t-testi)

Faktör analizi sonucunda belirlenen ve üç faktör altında toplanan 30 maddenin madde analizleri yapılmıştır. Analiz sonucunda madde-toplam test korelasyonları değerlerinin; çevrimiçi güvenlik farkındalığı faktöründe r=,65 ile r=,74 arasında, çevrimiçi merak faktörünün r=,57 ile r=,77 arası, siber tehdit farkındalığı faktöründe ise r=,64 ile r=,71 arası değişim gösterdiği belirlenmiştir. Madde-toplam korelasyonlarının ,30 ve üstü değer alması ölçek maddelerinin geçerliğine yönelik bir kanıt olarak görülmektedir (Nunnally ve Bernestein, 1994). Ölçekte yer alan 30 maddenin madde-toplam test korelasyonlarına bakıldığında her bir madde için r=,30'un üzerinde değer aldığı tespit edilmiştir. Elde edilen bu bulgu, ölçekte bulunan maddelerin ölçülmek istenen niteliği ölçme amacına yardımcı olduğunun göstergesidir. Ölçeğin t-testi sonuçları incelendiğinde ise %27 üst ve alt grupların madde puanları arasındaki farklara ilişkin t değerlerinin 2,54 ile 17,15 arasında değişim gösterdiği ve tüm maddelerin anlamlı olduğu görülmektedir (p<,001). Ayrıca üst %27 grubun bütün maddelere ait madde puan ortalamaları alt %27 gruba göre anlamlı bir şekilde yüksektir. Buna göre ölçekte bulunan her bir maddenin aynı davranışı ölçtüğü; yani ortaokul kademesinde öğrenim gören öğrencilere yönelik bilgi güvenliği farkındalık düzeyini ölçtüğü ve ölçeğin tümünde olduğu gibi alt faktörlerin de ayırt ediciliğinin yüksek olduğu

söylenebilir. Madde-toplam korelasyonları ile üst ve alt %27'lik gruplara ait madde ortalama puanları t-testi sonuçlarına göre ayırt ediciliği en yüksek maddenin 58. Ve en düşük maddenin ise 46. Madde olduğu tespit edilmiştir.

Güvenirlik Analizi: Ölçme aracının güvenirliğinin ortaya koyulması amacıyla Cronbach Alfa iç tutarlılık katsayı değerine bakılmıştır. Genel olarak güvenilirlik katsayısının ,70 ve üzeri değer alması yeterli olarak değerlendirilmektedir (Nunnally, 1978). Ölçeği oluşturan 30 maddenin Cronbach Alfa iç tutarlılık katsayısı ,90 olarak belirlenmiştir. Ölçeğin alt faktörlerinim belirlenmesi amacıyla gerçekleştirilen Cronbach Alfa iç tutarlılık analiz değerleri ise; çevrimiçi güvenirlik farkındalığı faktörü için ,94, çevrimiçi merak faktörü için ,90 ve siber tehdit farkındalığı faktörü için ,86 olarak ortaya çıkmıştır. Buna göre faktörlerin Cronbach Alfa iç tutarlılık katsayısı ,70'ten yüksek olduğu tespitinde yola çıkarak ölçeğin güvenilir ve tutarlı bir ölçek olduğu sonucuna ulaşılmıştır (Nunnally, 1978; Tavşancıl, 2005).

Doğrulayıcı Faktör Analizi: Çalışmanın AFA aşaması sonrası ortaya çıkan modele ilişkin yapı geçerliğinin değerlendirilmesi amacıyla DFA yapılmış (Kline, 2000) ve 30 maddeden oluşan üç faktörlü yapıya ilişkin DFA aşaması 265 öğrenci ile gerçekleştirilmiştir. Çalışmada model uyum indekslerinden; Ki-Kare İyilik Uyumu (χ2/df), İyilik Uyum İndeksi (GFI), Düzenlenmiş İyilik Uyum İndeksi (AGFI), Yaklaşık Hataların Ortalama Karekökü (RMSEA), Standardize Edilmiş Artık Ortalamaların Karekökü (SRMR), Karşılaştırmalı Uyum İndeksi (CFI), Normlaştırılmış Uyum İndeksi (NFI) ve Normlaştırılmamış Uyum İndeksi (NNFI) göz önünde bulundurulmuştur.

Ölçeği oluşturan 3 faktörlü yapıya ilişkin DFA sonrası model üzerinde önerilen modifikasyonlar yapılmadan önce ortaya çıkan uyum iyiliği indeksleri şöyledir: [χ2/df= 2,152 (p=,000); GFI= ,83; AGFI= ,80; RMSEA= ,066; SRMR= ,000; CFI= ,89; NFI= ,82; NNFI= ,89]. Analiz sonucu ortaya çıkan modifikasyon önerileri dikkate alındığında M6 ve M5; M17 ve M16; M19 ve M18; M23 ve M19; M24 ve M17; M24 ve M23; M8 ve M2; M9 ve M7; M11 ve M10; M12 ve M9; M14 ve M8; M14 ve M9 maddeleri arasında 12 modifikasyon önerisinin ortaya çıktığı görülmektedir. Alanyazın incelendiğinde; maddeler

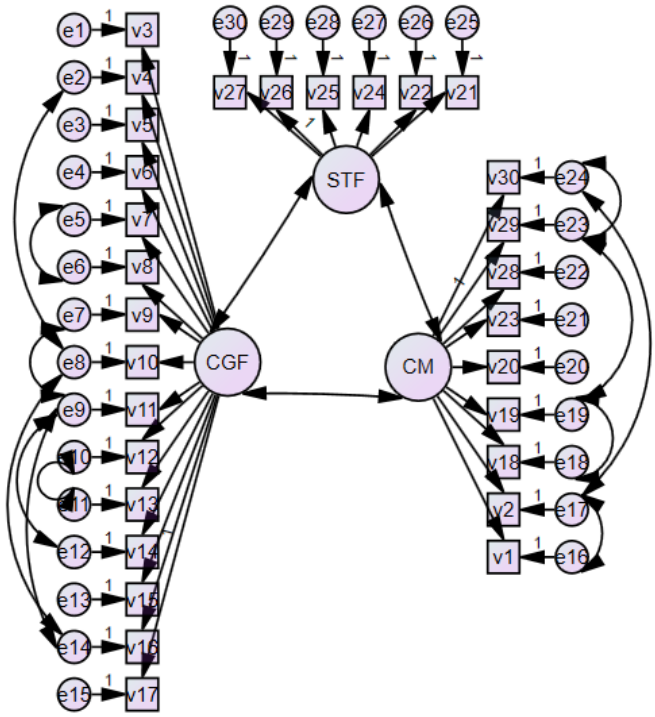
arasında gizil bir bağlantının olabileceği ve maddelerin benzer durumları, ölçtükleri göz önünde bulundurularak modifikasyona yönelik öneri dikkate alınmıştır. Modifikasyon ardından ortaya çıkan uyum indeksleri Tablo 11'de sunulmuştur (Jöreskog ve Sörbom, 1993; Schermelleh-Engel vd., 2003).

Tablo 12

Standart uyum iyiliği ölçütleri ile araştırma sonuçlarının karşılaştırılması

Uyum Ölçüleri	İyi Uyum	Kabul Edilebilir Uyum	Uyum değerleri
χ2/df	0≤ χ2/df ≤2df	2df≤ χ2/df ≤3df	1,52
RMSEA	0≤ RMSEA ≤0,05	0,05<RMSEA ≤0,10	,044
SRMR	0≤ SRMR ≤0,05	0,05< SRMR ≤0,10	,00
NFI	0,95< NFI ≤1,00	0,90 ≤ NFI <0,95	,88
NNFI	0,95≤ NNFI ≤1,00	0,90≤ NNFI ≤0,95	,95
CFI	0,95≤ CFI ≤1,00	0,90≤ CFI ≤0,95	,95
GFI	0,95≤ GFI ≤1,00	0,90≤ GFI <0,95	,88
AGFI	0,90≤ AGFI ≤1,00	0,85≤ AGFI <0,90	,85

Tablo 12'deki DFA sonuçlarına göre, ki-kare χ2 = 586; (df=386, p<,01); (χ2/df) = 1,52 olarak bulunmuştur. Küçük örneklemler için 2,5 ve altı değer alan modelleri mükemmel uyumlu olarak nitelendirmektedir (Çokluk vd., 2010; Kline, 2005). Diğer taraftan yapılan analizler sonucunda RMSEA=,044; SRMR=,00; GFI=,88; AGFI=,85; NFI=,88; CFI=,95 ve NNFI=,95 olarak bulunmuştur. Araştırmada elde edilen uyum indeks değerleri göz önüne alındığında χ2 /df, RMSEA, SRMR, NNFI ve CFI iyi uyumu, AGFI uyum indeksi kabul edilebilir uyumu ancak GFI, NFI, uyum indeksleri ise yakın olmakla birlikte zayıf uyum gösterdiği görülmektedir. Şimşek (2007), uyum indekslerinin aldıkları değerlerin örneklem büyüklüğünden etkilenebildiklerini belirtmiştir. Bütüncül bir değerlendirme yapıldığında uyum indeks değerlerinin iyi uyumu gösterdiği görülmektedir. Buna göre ortaya konan modelin doğrulandığı görülmektedir. Ölçeğin faktöriyel modeli şekil 5'te sunulmuştur.



Şekil 5. Ölçeğin birinci düzey doğrulayıcı faktör analizi bağlantı diyagramı

Ölçek maddelerine ait elde edilen çoklu korelasyon katsayı (t ve R^2) değerleri Tablo 12'de sunulmuştur. Üç faktörlü yapıya ait t değerleri göz önünde bulundurulduğunda gözlenen değişkenlerin, gizil değişken tarafından ,01 anlamlılık düzeyinde olduğu öngörülmektedir.

Tablo 13

Maddelere ilişkin çoklu korelasyon katsayısı (t ve R^2) değerleri

F1	Madde	t	R^2	F2	Madde	t	R^2	F3	Madde	t	R^2
Çevrimiçi Güvenlik Farkındalığı	S3	8,53	,33	Çevrimiçi Merak	S1	12,25	,64	Siber Tehdit Farkındalığı	S21	8,55	,39
	S4	7,68	,26		S2	11,58	,60		S22	7,34	,27
	S5	9,89	,45		S18	10,65	,48		S24	9,66	,53
	S6	10,09	,47		S19	10,31	,45		S25	9,11	,45
	S7	10,83	,55		S20	13,40	,77		S26	11,28	,51
	S8	10,27	,49		S23	11,96	,60		S27	9,74	,44
	S9	10,79	,55		S28	12,06	,62				
	S10	8,49	,32		S29	15,93	,78				
	S11	10,17	,48		S30	12,66	,50				
	S12	9,66	,43								
	S13	10,40	,51								
	S14	9,98	,46								
	S15	9,37	,40								
	S16	10,88	,45								
	S17	9,88	,46								

Alanyazın incelendiğinde önemli olan bir şart ise gözlenen değişkenin adına açıklanan varyansı ifade eden ve gözlenen değişkenin gizil değişkendeki farkı ne seviyede açıklayabildiği R^2 değeri ile ortaya koyulmaktadır (Şimşek, 2007). Yapıya ait değerler sonucunda bilgi güvenliği farkındalık düzeyine en yüksek katkıyı sırasıyla 29, 20, 1, 28 ve 23. Maddelerin, en düşük katkıyı ise sırasıyla 22, 10, 4, 3, ve 21. Maddelerin verildiği gözlemlenmektedir. Ortaya çıkan bu bulgu, açımlayıcı faktör analizinde ortaya çıkan bulguları desteklemektedir.

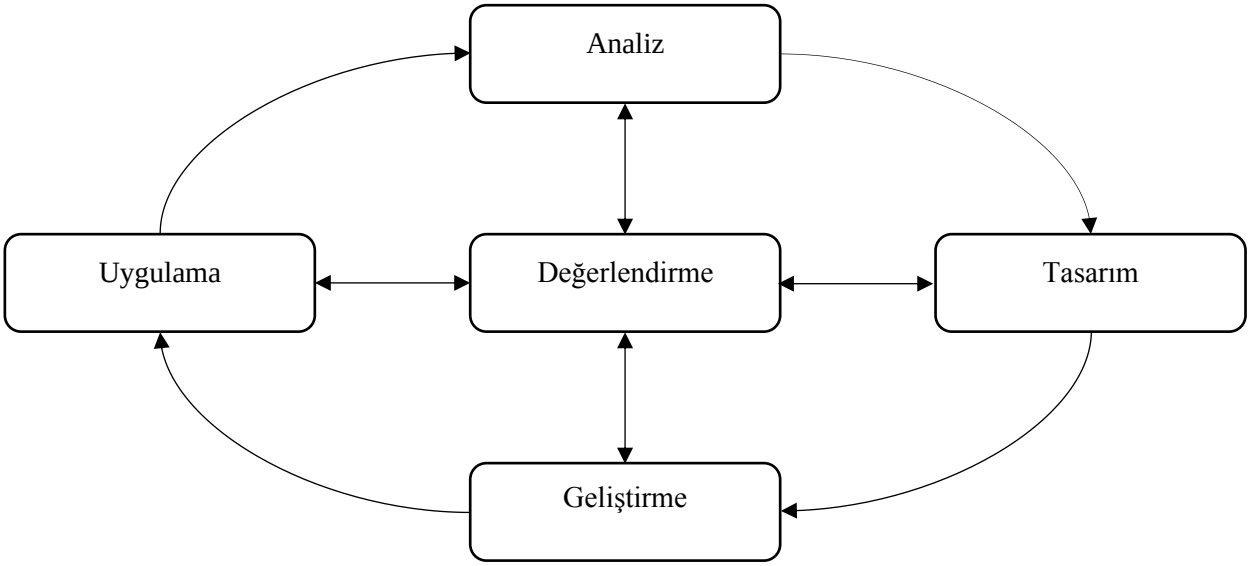
3.3.2. Görev Temelli Çevrimiçi Öğrenme Ortamının Oluşturulması

Çalışma kapsamında araştırmanın çalışma grubu özellikleri incelendiğinde öğrencilerin ortaokul düzeyinde oldukları görülmekte ve çalışma grubu gelişim ve öğrenme (teknoloji kullanımına ilişkin hazırbulunuşluk düzeyleri vb.) özellikleri açısından değerlendirilmiştir. Çalışma grubunun bu özellikler çerçevesinde incelenmesi içeriğin belirlenmesinde ve çoklu öğrenme ortamının tasarlanmasında (kullanım kolaylığı, amaca uygunluk vb.) rehber olmuştur. Araştırma grubunun gerek yaşları gerekse birinci sınıftan itibaren bilişim teknolojileri dersleri görmeleri ve hazırbulunuşluk düzeyleri incelendiğinde

öğrenme ortamının bilgisayar tabanlı olarak geliştirilmesinde bir sakınca görülmemiştir. Öğretim ortamlarının tasarım süreci incelendiğinde, birçok öğretim ortamı tasarlama modeli olduğu görülmektedir. Yapılandırmacı yaklaşımı esas alan tasarımlarda öğrenenin merkeze alındığı, öğrenenin öğrenme ortamında aktif olduğu ve işbirlikli öğrenmeyi destekleyen bir yapıya sahip oldukları görülmektedir. Bu yaklaşımları esas alan öğretim tasarımlarının geneli ise; analiz (analyze), tasarım(design), geliştirme(development), uygulama(implementation) ve değerlendirme(evaluation) olmak üzere 5 aşamadan oluşmaktadır (McGriff, 2000; Kaminski, 2007). Modellerden en fazla tercih edilen ADDIE modelinin (Reiser ve Dempsey, 2007) daha çok tercih edilmesinin en önemli nedeni ise her türlü öğrenim için temel bir model olmasıdır (Cheung, 2016).

ADDIE Modeli Bileşenleri

ADDIE modeli 1970'lerin sonunda Florida State University, Eğitim Teknolojisi Merkezi'nde geliştirilmiştir. ADDIE modeli bileşenleri şekil 6'da görüldüğü üzere analiz (analyze), tasarım(design), geliştirme(development), uygulama(implementation) ve değerlendirme(evaluation) bileşenlerinden oluşmaktadır (Allen, 2006; Branch, 2016; Kaminski, 2007; McGriff, 2000; Muruganantham, 2015).



Şekil 6. ADDIE modeli bileşenleri (Branch, 2016)

Analiz Bileşeni: Analiz bileşeni "hedef belirleme bileşeni" olarak düşünebilir. Bu aşamada tasarımcının odak noktasında hedef kitle vardır. Ayrıca öğretim tasarımının her öğrenenin gösterdiği beceri ve zekâ düzeyiyle eşleştiği aşamadır. Analiz bileşeni diğer tüm bileşenlerin temelini oluşturmaktadır. Sistem analizi yapılarak problem tanımlanır, kısıtlamalar belirlenir ve olası çözümler geliştirilir. Bunun yanı sıra bu aşamada öğrenen profili, gelişim düzeyleri, eğitim seviyeleri belirlenmiş olmaktadır. Aşağıda analiz aşamasında ele alınan bazı sorulara yer verilmiştir.

- Hedef kitle kimdir ve özellikleri nelerdir?
- Hedef kitle öğretimin sonunda neyi başarmaları gerekiyor? Hedef kitlenin ihtiyaçları nelerdir?
- Öğrenme sürecinin sınırlılıkları nelerdir?
- Öğretim tasarımının tamamlanması için zaman çizelgesi nedir?

Bu aşamada elde edilen veriler ile tasarım sürecine geçilir (Allen, 2006; Muruganantham, 2015).

Tasarım Bileşeni: Analiz aşamasında elde edilen veriler sonrası bu aşama tüm hedeflerin, performansı ölçmek için kullanılacak araçların, konu analizlerinin, öğretim süreci planlamasının ve kullanılacak olan kaynakların belirlendiği aşamadır. Bu aşamada proje hedeflerine ulaşmak için oluşturulan stratejilerin mantıklı olması, açık bir şekilde tanımlanması, geliştirilmesi ve değerlendirilmesi sistematik olmalıdır. Öğretim tasarımı sürecinin her bir unsurunun ayrıntılarına dikkat edilmelidir. Aşağıda tasarım aşamasında ele alınan bazı sorulara yer verilmiştir.

- Kullanılacak medya türleri (ses, video vb.) nelerdir?
- Projeyi tamamlamak için mevcut kaynaklar yeterli midir?
- Öğretim tasarımını amacına uygun mudur? Kullanılacak olan yaklaşım nedir?
- Öğretim ortamında geri bildirimlerini almak için nasıl bir yol izlenir? (Allen, 2006; Muruganantham, 2015).

Geliştirme Bileşeni: Geliştirme aşaması önceki iki aşamadan toplanan veriler ile içerik ve materyallerin hazırlanma aşamasıdır. Bu aşamanın amacı materyali geliştirmektir.

Bu aşamada taslak hazırlama, üretim ve değerlendirme olarak üçe ayrılmaktadır. Aşağıda geliştirme aşamasında ele alınan bazı sorulara yer verilmiştir.

- Materyal zaman çizelgesine bağlı kalarak mı hazırlanıyor?
- Öğrenenler arasında iş birliği var mıdır? Öğrenenler etkin bir şekilde sürece dahil olmakta mıdır?
- Kaynaklar amaçlanan materyale uygun mudur? (Allen, 2006; Muruganantham, 2015).

Uygulama Bileşeni: Öğretim tasarımının öğrenenler ile tam olarak uygulamaya koyulmasıdır. Bu aşamanın amacı öğretim materyalinin maksimum verimlilik ile sunulmasıdır. Bu aşamada öğrenenlerden gelen geribildirimlere göre materyalin eksiklikleri ve iyi yönleri belirlenir. Belirlenen eksiklikler giderilerek öğrenenlere uygun bir tasarım gerçekleştirilir (Allen, 2006; Muruganantham, 2015).

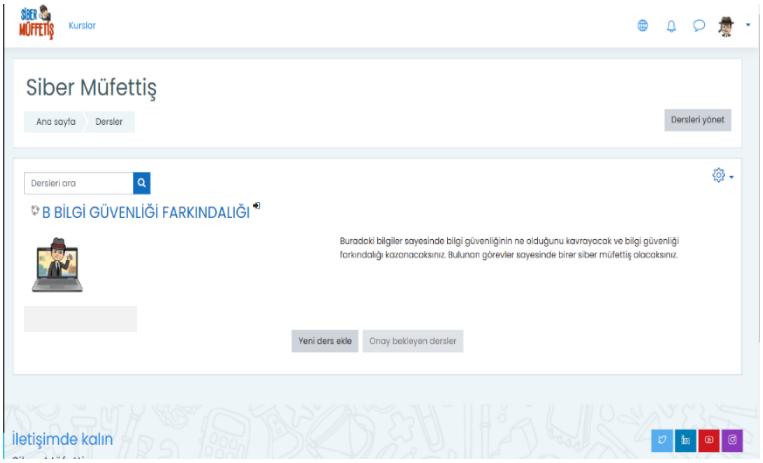
Değerlendirme Bileşeni: ADDIE modelinin son aşamasıdır. Materyalin yeterliliğinin ve etkisinin incelendiği aşamadır. Değerlendirme aşaması biçimlendirici ve düzey belirleyici olarak ikiye ayrılır. Biçimlendirici aşamasında ADDIE modelinin her aşamasında gerçekleşen değerlendirmedir. Düzey belirleyici değerlendirme ise materyalin sonunda gerçekleşir. Değerlendirme aşaması, hedeflere ulaşılıp ulaşılmadığını belirlemek, materyalin verimliliğini ve başarı oranını daha da arttırmak için hangi düzenlenmeleri gerekli olacağının belirlendiği aşamadır (Allen, 2006; Muruganantham, 2015).

Öğretim Materyali ve Materyalin Genel Özellikleri

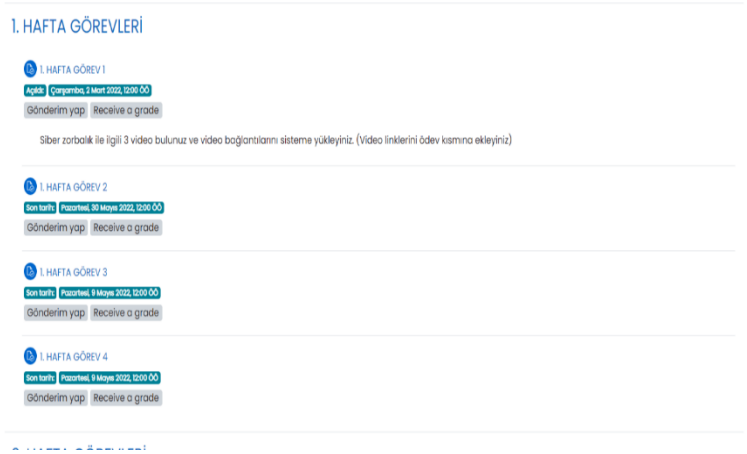
Öğretim materyali ADDIE modelinde bulunan aşamalar esas alınarak hazırlanmıştır. Hedef kitlenin 10-14 yaş aralığında olması nedeniyle kullanım kolaylığı ve motivasyonu sağlayacak tasarım ilkelerinden faydalanılmıştır. Tasarlanan öğretim materyali öğrenen merkezli olarak hazırlanmıştır. Öğrenciler görev temelli çevrimiçi öğrenme ortamına giriş yaptığında öğrencileri ve sürecin sağlıklı yürütülmesini destekleyen yönergeler bulunmaktadır. Web tabanlı ortamın isminin belirlenmesinde öğrenci görüşlerine yer

verilerek uzmanlar tarafından “siber müfettiş” olarak belirlenmiş ve moodle eğitim yazılımı kullanılarak hazırlanmıştır. Moodle, kullanım kolaylığı, ücretsiz, açık kaynak kodlu ve çoklu dil desteği olan dünyada en çok kullanılan öğretim yönetim sistemi yazılımdır (Başaran, 2010). Moodle destekli olarak hazırlanan öğretim materyalinde zaman tasarrufu sağlamak amacıyla elektronik ortamda öğrenci ad, soyad ve e-posta bilgilerine göre sistematik olarak her öğrenciye bir kullanıcı adı ve şifre tanımlanmıştır. Daha sonra öğrencilere kullanıcı adı ve şifreleri e-posta yoluyla paylaşılmıştır. Web tabanlı öğretim materyalini yüz yüze eğitime ek olarak web üzerinden eş zamanlı (senkron) ve eş zamansız (asenkron) kullanıma olanak sağlanmıştır. Şekil 7, Şekil 8 ve Şekil 9’da öğretim materyaline ait fotoğraflar sunulmuştur.

Şekil 7. Görev temelli öğrenme ortamı ana sayfası



Şekil 8. Görev temelli öğrenme ortamı bilgi güvenliği farkındalığı kurs giriş sayfası



Şekil 9. Görev temelli öğrenme ortamı görevlerin bulunduğu sayfa

3.3.3. Görevlerin Belirlenmesi ve Uygulama Süreci

Araştırmada katılımcıların bilgi güvenliği farkındalıklarını sağlamada sunulacak olan görev zorlukları için Newcomb ve Treftz (1987) tarafından ortaya konulan model esas alınarak belirlenmiştir. Hatırlama seviyesinde bulunan görevler "çok kolay", işleme seviyesindeki görevler "kolay", oluşturma seviyesindeki görevler "zor" ve değerlendirme seviyesindeki görevler ise "çok zor" olarak göz önünde bulundurulmuştur.

Tablo 14

Görevlerin zorluk seviyelerinin belirlenmesinde kullanılan yaklaşım

Newcomb- Treftz Modeli	**Görev Zorluk Seviyesi**
Hatırlama (Remembering)	Çok Kolay
İşleme (Processing)	Kolay
Oluşturma (Creating)	Zor
Değerlendirme (Evaluation)	Çok Zor

Bu modele göre; hatırlama (çok kolay) seviyesi, bir konu hakkındaki kavramların, sınıflamaların, ölçütlerin ve çözümlerin tanınmasını veya hatırlanmasını ile ilgilidir. Herhangi bir kavramla ilgili özellikleri görünce tanıması ya da ezberden aynen tekrar etmesi davranışlarını kapsamaktadır. Belli bir kavramın en önemli nitelikleri ve iki kavram arasındaki ana farklar gibi bilgi öğeleri bu zorluk seviyesinde düşünülür. İşleme (Kolay) seviyesinde, hatırlama seviyesinde elde edilen bilgi ve yeteneklerin öğrenci tarafından benimsenmesi söz konusudur. Öğrenilen bilgilerin yeni bir şekilde, yeni bir düzenlemeyle

sunması veya farklı şekillerde ve karşılaştığında onları tanıması istenir. Parçalar arasındaki bağı görüp anlam kazandırmayı içerir. Yapılan aktivitelerle alakalı neden sonuç ilişkilerini, öncelik sonralık bağlantılarını ayırt etmesi gerekir. Oluşturma (Zor) seviyesinde, belirli bir amaca yönelik öğeleri seçip onları belirli kavramlara ve kurallara göre ilişkilendirip birleştirerek yeni bir öğe ortaya çıkarması gerekir. Bu seviyede öğrencilerden özgünlük beklenmektedir. Öğrencinin yaratıcılığını göstermesini sağlayacak görevler olmalıdır. Değerlendirme (Çok Zor) seviyesinde ise, belirli bir hedefe yönelik olarak belirli kurallar yardımcıyla bir kavramın değerini bilinçli bir şekilde yargılamayı içermektedir. Bu seviyede öğrenciler, yöntemler, fikirler ve çözüm yolları hakkında yargılar verebilir. Oluşturulan görevlerin kapsam geçerliği için bir form hazırlanarak bilgisayar ve öğretim teknolojileri eğitimi anabilim dalında görev yapan beş öğretim elemanı ve bilişim teknolojileri öğretmenliği yapmakta olan üç bilişim teknolojileri öğretmeni olmak üzere sekiz uzmana gönderilmiştir. Bu formda uzmanlar görevleri zorluk düzeyine göre değerlendirmişlerdir. Gelen geri bildirimlerin ardından gerekli düzenlemeler yapılarak görevler son halini almıştır (EK7).

Beş haftalık uygulama sürecinin ilk haftasında, çalışmaya katılan öğrencilerin bilgi güvenliği farkındalıklarını ölçmek ve deney ve kontrol grupları arasında farklılık olup olmadığını belirlemek amacıyla araştırmacı tarafından hazırlanmış olan ortaokul düzeyi bilgi güvenliği farkındalığı ölçeği öntest olarak uygulanmıştır. Öntest sonucunda gruplar arasında bilgi güvenliği farkındalığı arasında farklılığın olmadığı görülmüştür. Ardından başlayacak olan uygulama süreci ile ilgili genel bilgiler verilmiştir. Uygulama sürecinin ikinci haftasında ise; uygulama süreci başlamadan önce öğrencilere öğretim materyaline ilişkin genel bilgilendirme, öğretim materyalinin nasıl kullanılacağı ile ilgili bilgi paylaşımı yapılmıştır. Daha sonra araştırmacı tarafından sistematik bir şekilde oluşturulan kullanıcı adı ve şifreleri öğrenciler ile paylaşılmıştır. Ardından öğrenciler kendilerine verilen kullanıcı adı ve şifreleriyle web tabanlı öğretim materyaline giriş yapmışlardır. Öğrenciler hem web tabanlı öğretim materyalinin arayüzünü incelemiş hem de haftanın görevlerini yapmaya başlamışlardır. Yaptıkları her görev sonrası araştırmacı tarafından öğrencilere 0-100 arası bir puanlama yapılmıştır. Geçer not alan öğrenciler bir sonraki göreve geçmiş, geçer not almayan öğrenciler ise geçer not alabilene kadar aynı görevi farklı bir şekilde yapmışlardır. Uygulama sürecinin üçüncü haftasında ise; öğrenciler kendilerine verilen kullanıcı adı ve

şifreleriyle araştırmacı tarafından hazırlanan web tabanlı öğretim materyaline giriş yapmışlardır. Geçen haftada olduğu gibi öğrencilere atanmış olan ikinci hafta görevlerini inceleyerek görevleri tamamlamışlardır. Bir önceki haftada olduğu gibi araştırmacı tarafından öğrencilerin yaptıkları görevler sonrası öğrencilere 0-100 arası bir puanlama yapılmıştır. Sonrasında öğrenciler bir sonraki haftaya hazırlıklarını gerçekleştirmişlerdir. Uygulama sürecinin dördüncü haftasında ise; öğrenciler üçüncü hafta görevleri için web tabanlı öğretim materyaline giriş yapmışlardır. Üçüncü hafta görevlerini tamamlamışlar ve araştırmacı tarafından verilen puanlar ile bir sonraki göreve geçiş yapmışlardır. Uygulama sürecinin beşinci haftasında ise; son görev haftasında bulunan dört görevi tamamlamak için öğrencilere verilen kullanıcı adı ve şifreyle web tabanlı öğretim materyaline giriş yapmışlardır. Daha sonra öğrenciler son haftaya ait olan görevleri tamamlamışlar ve araştırmacı tarafından yapılan puanlamaların ardından deneysel sürecinin sonunda bilgi güvenliği farkındalık düzeylerinin incelemek amacıyla sontest gerçekleştirilmiştir. Uygulama süreci tamamlandıktan sonra deney grubu öğrencilerinin uygulama süreci boyunca kullandıkları görev temelli çevrimiçi öğrenme ortamı hakkında açık uçlu soru formu teslim edilmiştir. Bu form sayesinde öğrencilerin öğretim materyali hakkında görüşleri alınıp içerik analizi ile çözümlenmiştir.

Uygulama süreci boyunca her hafta dört farklı görev zorluk seviyesinde olmak üzere öğrencilere toplam 16 görev verilmiştir. Bu görevler uygulamalı ve öğrencilerin merkez alındığı görevlerden oluşmaktadır. Öğrenciler her bir görev için 0-100 arasında puan almışlardır. Öğrenciler geçerli not olan 70 üzeri puan sayesinde görevi tamamlamış sayılıp bir sonraki göreve geçmeye hak kazanmıştır. Öğrenciler her tamamladıkları üç görev sonrası sırasıyla “acemi müfettiş”, “çaylak müfettiş”, “uzman müfettiş”, “usta müfettiş” ve “efsane müfettiş” nişanlarını almaya hak kazanmışlardır. Tüm görevleri başarıyla tamamlayan öğrenciler ise “siber müfettiş” nişanı alarak kursu başarıyla tamamlamışlardır. Öğrencilere verilen görevler sayesinde öğrenciler kendisindeki ilerlemeyi görebilecektir. Bunun yanı sıra görevler gerçek hayatta karşılaşacağı olaylardan oluştuğu için öğrencinin motivasyonunu artıracağı düşünülmektedir. Alanyazında ödül/ceza eğitim alanında en çok kullanılan eğitim yöntemlerinden biri olarak görülmekte olup, davranışçı yaklaşıma göre hayvanlar üzerinde etkinli olan edimsel koşullanmanın (eğitimde ödül/ceza uygulamaları) çocuk yetiştirmede de etkili olacağı düşünülmektedir (Cüceoğlu, 2015). Çolak’a (2005) göre öğrencilerin

gösterdikleri sorumluluk alma, iş birliği yapma, başarılı olma ve etkinliklere katılma gibi durumların büyük bir bölümü iyi bir motivasyon kaynaklıdır.

3.4. Veri Toplama Araçları ve Veri Toplama Süreçleri

Bu kısımda, veri toplama araçları, araştırmanın uygulama süreci, geliştirilen çevrimiçi öğrenme ortamı, verilerin toplanması ve veri analizi ile ilgili bilgilere yer verilmiştir.

3.4.1 Verilerin Toplama Araçları

Bu araştırmanın verileri; ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeylerini tespit etmek amacıyla araştırmacı tarafından geliştirilen EK1'deki "Ortaokul Düzeyi Bilgi Güvenliği Farkındalık Ölçeği" ve EK2'deki çevrimiçi görev temelli ortamına yönelik ortaokul öğrencilerinin tutumlarını incelemek amacıyla araştırmacı tarafından oluşturulan açık uçlu soru formu kullanılmıştır. Bu çerçevede çalışmada kullanılan ölçme araçlarına yönelik detaylı bilgi aşağıda sunulmuştur.

Ortaokul Düzeyi Bilgi Güvenliği Farkındalığı Ölçeği

Çalışmada, ilköğretim düzeyi ortaokul kademesinde öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemek amacıyla alanyazında hedef kitle özelliklerini karşılayan ölçek bulunmadığından dolayı araştırmacı tarafından geliştirilen 30 madde ve 3 alt boyuttan (çevrimiçi güvenlik farkındalığı, çevrimiçi merak, siber tehdit farkındalığı) oluşan "Ortaokul Düzeyi Bilgi Güvenliği Farkındalığı Ölçeği" kullanılmıştır (bkz., bölüm 3.3.1).

Açık Uçlu Soru Formu

Çalışmaya katılan öğrencilerin araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamına ve sürecine ilişkin görüşlerin belirlenmesi amacıyla açık uçlu soru formu hazırlanmıştır. Hazırlanan form kapsam geçerliliği açısından uzmanlara inceletilmiş ve gerekli düzenlemeler sonrasında ölçme aracına son hali verilmiştir. Gerekli düzenlemeler ile birlikte son halini alan veri toplama aracındaki açık uçlu soru formunda bulunan sorular aşağıdaki gibidir:

1. Geliştirilen Görev temelli çevrimiçi öğrenme ortamına yönelik görüşleriniz nelerdir? Açıklayınız.
2. Görev temelli çevrimiçi öğrenme ortamında eğitim aldığınız sürece yönelik görüşleriniz nelerdir? Açıklayınız.

Oluşturulan form uygulama süreci sonrasında deney grubundaki öğrencilere elektronik ortamda sunulmuştur. Deney grubundaki öğrencilerin geliştirilen öğrenme ortamına yönelik görüşleri öğrenme ortamı değerlendirme formuna verilen yanıtlar doğrultusunda analiz edilmiştir.

3.5. Verilerin Analizi

Araştırmada elde edilen veriler Office Excel ile düzenlenerek bilgisayar ortamında SPSS 26.0, LISREL ve SPSS AMOS istatistik paket programları ile aktarılmıştır. Araştırmanın uygulama aşamasının ilk bölümünde, ortaokul bilgi güvenliği farkındalık ölçeğini geliştirmek ve elde edilen verileri analiz etmek amacıyla istatiksel çalışmalar yapılmıştır. İlk adımda 124 maddeyi içeren soru havuzu oluşturulmuş ardından kapsam geçerliği çalışması için 9 uzmana gidilmiştir. Uzman değerlendirmesi sonrasında 20 madde havuzdan çıkarılmıştır. Kapsam geçerliği sonrası 104 maddeden oluşan ölçek ilköğretim düzeyi ortaokul kademesinde öğrenim gören öğrencilere uygulanmıştır. Araştırmada elde edilen verilerin açımlayıcı faktör analizine uygunluğunun saptanması amacıyla; Kaiser-Meyer-Olkin (KMO) ile birlikte Barlett Küresellik testi ölçümlerinden faydalanılmıştır. Faktörlerin açıkladığı varyans değerine ve varimax dik döndürme tekniği kullanılarak

maddelerin faktörlere göre dağılımları incelenmiştir. Alt üst %27'lik grupların ortalamaları t-testi ile sınanarak madde ayırt edicilik analizleri yapılmıştır. Bu analizlerin sonrasında ölçeğin iç tutarlılığını belirlenmesi için Cronbach Alpha güvenirlik analizi yapılmıştır. İç tutarlılık analizinden sonra ortaya çıkan modele ilişkin yapı geçerliğinin değerlendirilmesi amacıyla doğrulayıcı faktör analizi yapılmıştır.

Araştırmanın uygulama aşamasının ikinci bölümünde, ortalama, çarpıklık ve basıklık katsayıları ve mod medyan analizleri yapılmıştır. Verilerin homojenliğinin tespit edilmesi amacıyla Levene Testi uygulanmıştır (Büyüköztürk, 2010). Deney ve kontrol grubu öğrencilerinin yarı deneysel işlem öncesinde öntest bilgi güvenliği farkındalık düzeyi puanları arasında istatiksel olarak anlamlı bir farklılık olup olmadığına ilişkin bağımsız gruplar t testi yapılarak test edilmiştir. Deney ve kontrol grubu öğrencilerinin öntest ve sontest aşamasında aldıkları bilgi güvenliği farkındalık düzeyi puanları ve alt faktörlerden aldıkları puanlar arasında anlamlı bir farklılık olup olmadığı bağımlı gruplar t testi yapılarak test edilmiştir. Deneysel süreç sonucunda deneysel işlemin gruplar üzerindeki etkisini belirlemek amacıyla öntest bilgi güvenliği farkındalık puanları kontrol edilerek, sontest bilgi güvenliği farkındalık puanları ile karşılaştırılması için kovaryans (ANCOVA) analizi yapılmıştır. Kovaryans analizine genellikle öntest-sontest kontrol gruplu desenlerde, deney ve kontrol grubunun sontest ölçümleri arasında anlamlı bir farkın olup olmadığını test etmek için başvurulmaktadır ve öntest ölçümleri ortak değişken olarak tanımlanmaktadır (Büyüköztürk, 2010). Araştırmanın nitel boyutunda ise ortaokul öğrencilerinin görev temelli çevrimiçi öğretim materyali hakkında görüşlerini incelemek amacıyla içerik analizi türlerinden kategorisel analiz ve frekans analizi kullanılmıştır. İçerik analizi, belirli kurallara dayalı kodlamalarla bir metnin bazı sözcüklerinin daha küçük içerik kategorileri ile özetlendiği sistematik, yinelenebilir bir teknik olarak tanımlanmaktadır (Büyüköztürk vd., 2016). İçerik analiz türlerinden biri olan kategorisel analiz sürecinde veriler, verilerin kodlanması, kategorilerin oluşturulması, kategorilerin düzenlenmesi, bulguların tanımlanması ve yorumlanması aşamaları izlenerek analiz edilmektedir (Corbin ve Strauss, 2007). Frekans analizinde ise veriler sayısal anlamda ortaya koyularak, öne çıkan kavramlar belirlenmiştir (Tavşancıl ve Aslan, 2001). Bu doğrultuda, elde edilen verilerin güvenirliği ve geçerliliği arttırılmış, yanlılık azaltılmış ve veriler arasında karşılaştırma yapılması sağlanmıştır (Yıldırım ve Şimşek, 2011).

DÖRDÜNCÜ BÖLÜM
ARAŞTIRMA BULGULARI

Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeylerini arttırmaya yönelik görev temelli çevrimiçi öğrenme ortamı geliştirilmesi ve etkililiğinin belirlenmesi amaçlanan çalışmanın bu bölümünde toplanan nicel ve nitel verilerin istatistiksel çözümlemelerine ve elde edilen bulguların yorumlarına yer verilmiştir.

4.1. Nicel Verilere Yönelik Bulgular ve Yorumlar

4.1.1. Deney ve Kontrol Grubundaki Öğrencilerin Demografik Özelliklerine Ait Bulgu ve Yorumlar

Araştırmaya katılan deney ve kontrol grupları öğrencilerinin demografik özellikleri; cinsiyet değişkeni açısından incelenmiştir. Deney ve kontrol gruplarındaki öğrencilerin cinsiyete göre dağılımı Tablo 15'te sunulmuştur.

Tablo 15

Deney ve kontrol grubu öğrencilerinin cinsiyete göre dağılımı

	Deney Grubu		**Kontrol Grubu**		**Toplam**	
Cinsiyet	N	%	N	%	**N**	**%**
Kız	8	%40	9	%45	**17**	**%42,5**
Erkek	12	%60	11	%55	**23**	**%57,5**
Toplam	**20**	**%100**	**20**	**%100**	**40**	**%100**

Tablo 15 incelendiğinde araştırmanın deney ve kontrol grubunu oluşturan öğrencilerin (N=40) cinsiyete göre dağılımına bakıldığında; %57,5'lik kısmını erkek öğrencilerin (N=23) oluşturduğu %42,5'lik kısmını da kız öğrencilerin (N=17) oluşturduğu görülmektedir.

4.1.2. Deney ve Kontrol Grubu Öğrencilerinin Öntest Bilgi Güvenliği Farkındalık Düzey Puanlarına İlişkin Bulgu ve Yorumlar

Uygulama öncesi, iki grubun ön bilgilerinin belirlenmesi ve dağılımın homojenliğini kontrol etmek için öğrencilere öntest uygulanmıştır. Verilerin homejenliğinin sağlandığı ve normal dağılım gösterdiği, durumlarda parametrik testler uygulanır (Yılmaz, 2015; Öztuna ve Elhan, 2015). Bu doğrultuda, deney ve kontrol grubu öğrencilerinin öntest bilgi güvenliği farkındalık düzeyi puanlarının homejenliği sağlayıp sağlamadığı ve ilişkin Levene Testi uygulanmıştır. Deney ve kontrol gruplarına uygulanan öntest sonrasında, gruplar arasında homejenliğin sağlandığı (Levene Statistic F=0,833, p>,05) belirlenmiştir. Daha sonra verilerin normal dağılım gösterip göstermediğine ilişkin çarpıklık ve basıklık değerleri incelenmiştir. Tablo 16'da deney ve kontrol grubu öğrencilerinin öntest bilgi güvenliği farkındalık düzey puanlarına ait betimsel istatistikler sunulmuştur.

Tablo 16

Deney ve kontrol grubu öğrencilerinin öntest bilgi güvenliği farkındalık ölçeği değerlerinin betimsel istatistikleri

	N	**X̄**	**Ss**	**Çarpıklık**	**Basıklık**
Deney	20	128	17,06	-,998	,241
Kontrol	20	118,7	18,38	,345	-,618

Tabachnick ve Fidell (2013) çarpıklık ve basıklık verilerinin +1,5 ile -1,5 arasında bulunan değerlerin kabul edilebilir düzeyde olduğunu ve verilerin normal dağıldığını ifade etmektedir. Tablo 16 incelendiğinde deney grubu öğrencilerine ait öntest ölçüm değerlerinin çarpıklık (-,998) ve basıklık (,241) değerleri ile kontrol grubu öğrencilerine ait öntest ölçüm değerlerinin çarpıklık (,345) ve basıklık (-,618) değerleri göz önünde bulundurulduğunda verilerin normal dağılım gösterdiği söylenebilir. Çalışmanın gerçekleştirildiği sınıflar arasında homojenlik söz konusu olduğundan, dağılımın normallik varsayımını yerine getirmesinden ve iki grup olmasından dolayı, verilerin çözümlenmesinde bağımsız gruplar t testi analizi kullanılmıştır. Öğrencilerin öntest ve sontest aşamasında aldıkları bilgi güvenliği farkındalık düzeyi puanları arasında anlamlı bir farklılık olup olmadığına ilişkin gerçekleştirilen bağımsız gruplar t testi analizi sonuçları Tablo 17'da sunulmuştur.

Tablo 17

Deney ve kontrol grubundaki öğrencilerin bilgi güvenliği farkındalık düzeyi öntest puanlarına ilişkin bağımsız gruplar t testi sonuçları

	Grup	N	X̄	S	Sd	t	p*
Öntest	**Deney**	20	128	17,07	38	1,658	,106
	Kontrol	20	118,7	18,38			

*p<=,05

Tablo 17 incelendiğinde deney ve kontrol grubu öğrencilerinin bilgi güvenliği farkındalık düzeyi öntest puanları arasında anlamlı bir farklılığın olmadığı belirlenmiştir (t=1,658; p>,05). Bu doğrultuda uygulama öncesi deney ve kontrol gruplarının öntest bilgi güvenliği farkındalık düzeyi puanları arasında anlamlı bir farklılık bulunmadığı ve grupların öntest puanları göz önünde bulundurulduğunda homojenliğin sağlandığı ve verilerin normal dağıldıkları söylenebilir. Bu bulgu deney ve kontrol grubunu oluşturan öğrencilerinin birbirine denk olduğu şeklinde yorumlanabilir.

4.1.3. Deney ve Kontrol Grubu Öğrencilerinin Öntest-Sontest Bilgi Güvenliği Farkındalık Düzeyi Puanlarına İlişkin Bulgu ve Yorumlar

Geleneksel ortama ek olarak geliştirilen öğrenme ortamını kullanan deney grubu ve geleneksel ortamda öğrenim gören kontrol grubu öğrencilerinin öntest ve sontest aşamasında aldıkları bilgi güvenliği farkındalık düzeyi puanları ve alt faktörlerden aldıkları puanlar arasında anlamlı bir farklılık olup olmadığına ilişkin cevap aranmıştır. Deney grubu öğrencilerin öntest ve sontest aşamasında aldıkları bilgi güvenliği farkındalık düzeyi puanları ve alt faktörlerden aldıkları puanlar arasında anlamlı bir farklılık olup olmadığına bağımlı gruplar t testi yapılarak analiz sonucu Tablo 18'da sunulmuştur.

Tablo 18

Deney grubu öğrencilerinin bilgi güvenlik farkındalık ölçeği öntest ve sontest puanlarına ilişkin bağımlı örneklem t testi sonuçları

	N	X̄	S	Sd	t	P
Çevrimiçi Güvenlik Farkındalığı	20	62,35	10,56	19	-2,295	,033
	20	68	5,97			
Çevrimiçi Merak	20	39,70	4,54	19	-3,142	,005
	20	42,80	2,35			
Siber Tehdit Farkındalığı	20	25,95	3,30	19	-3,462	,003
	20	28,70	1,78			
Toplam	20	128	17,06	19	-2,958	,008
	20	139,5	8,88			

Tablo 18 incelendiğinde araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamında öğrenim gören deney grubu öğrencilerinin ölçeğin tamamından aldıkları öntest ve sontest bilgi güvenliği farkındalık düzeyi puanlarında anlamlı bir farklılığın olduğu belirlenmiştir (t=-2,958; p<,05). Deney grubunda yer alan öğrencilerin yarı deneysel işlem öncesi öntest puanları ortalaması X̄=128 iken, araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamı ile eğitim gördükten sonra bilgi güvenliği farkındalık düzeyi puanları ortalaması X̄=139,5'e yükselmiştir. Alt faktörler açısından incelendiğinde araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamında öğrenim gören deney grubu öğrencilerinin çevrimiçi güvenlik farkındalığı faktörü öntest ve sontest puanlarında anlamlı bir farklılığın olduğu görülmektedir (t=-2,295; p<,05). Deney grubunda yer alan öğrencilerin yarı deneysel işlem öncesi çevrimiçi güvenlik farkındalığı faktörü öntest puanları ortalaması X̄=62,35 iken, araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamı ile eğitim gördükten sonra çevrimiçi güvenlik farkındalığı faktörü puanları ortalaması X̄=68'e yükselmiştir. Çevrimiçi merak faktörü açısından incelendiğinde araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamında öğrenim gören deney grubu öğrencilerinin öntest ve sontest puanlarında anlamlı bir farklılığın olduğu görülmektedir (t=-3,142; p<,05). Deney grubunda yer alan öğrencilerin yarı deneysel işlem öncesi çevrimiçi merak faktörü öntest puanları ortalaması X̄=39,70 iken, araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamı ile eğitim gördükten sonra çevrimiçi merak faktörü puanları ortalaması X̄=42,80'e yükselmiştir. Siber tehdit farkındalığı faktörü açısından incelendiğinde araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamında öğrenim gören deney grubu öğrencilerinin öntest ve sontest

puanlarında anlamlı bir farklılığın olduğu görülmektedir (t=-3,462; p<,05). Deney grubunda yer alan öğrencilerin yarı deneysel işlem öncesi siber tehdit farkındalığı faktörü öntest puanları ortalaması $\bar{X}$=25,95 iken, araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamı ile eğitim gördükten sonra çevrimiçi merak faktörü puanları ortalaması $\bar{X}$=28,70'e yükselmiştir. Bu bulgulara göre araştırmacı tarafından geliştirilen öğrenme ortamının bilgi güvenliği farkındalık ölçeği ve alt faktörlerinin puanlarını arttırma konusunda önemli bir etkiye sahip olduğu söylenebilir. Deney grubuna yönelik yapılan analiz sonrası kontrol grubu öğrencilerin öntest ve sontest aşamasında aldıkları bilgi güvenliği farkındalık düzeyi puanları ve alt faktörlerden aldıkları puanlar arasında anlamlı bir farklılık olup olmadığına bağımlı gruplar t testi yapılarak analiz sonucu Tablo 19'da sunulmuştur.

Tablo 19

Kontrol grubu öğrencilerinin bilgi güvenlik farkındalık ölçeği öntest ve sontest puanlarına ilişkin bağımlı örneklem t testi sonuçları

	N	$\bar{X}$	S	Sd	t	P
Çevrimiçi Güvenlik Farkındalığı	20	57,95	10,42	19	-1,110	,281
	20	60,65	11,14			
Çevrimiçi Merak	20	36,65	5,13	19	-,785	,442
	20	37,65	5,94			
Siber Tehdit Farkındalığı	20	24,10	4,10	19	-1,244	,228
	20	25,25	3,99			
Toplam	20	118,7	18,38	19	-1,312	,205
	20	123,65	17,90			

Tablo 19 incelendiğinde geleneksel yöntem ile öğrenim gören kontrol grubu öğrencilerinin bilgi güvenliği farkındalık düzeyi puanlarında anlamlı bir farklılığın olmadığı belirlenmiştir (t=-1,312; p>,05). Kontrol grubunda yer alan öğrencilerin yarı deneysel işlem öncesi öntest puanları ortalaması $\bar{X}$=118,7 iken, geleneksel yöntem ile eğitim gördükten sonra bilgi güvenliği farkındalık düzeyi puanları ortalaması $\bar{X}$=123,65'e yükselmiştir. Alt faktörler açısından incelendiğinde geleneksel yöntem ile öğrenim gören kontrol grubu öğrencilerinin çevrimiçi güvenlik farkındalığı faktörü öntest ve sontest puanlarında anlamlı bir farklılığın olmadığı görülmektedir (t=-1,110; p>,05). Kontrol grubunda yer alan öğrencilerin yarı deneysel işlem öncesi çevrimiçi güvenlik farkındalığı faktörü öntest

puanları ortalaması $\bar{X}$=57,95 iken, deneysel yöntem ile eğitim gördükten sonra çevrimiçi güvenlik farkındalığı faktörü puanları ortalaması $\bar{X}$=60,65'e yükselmiştir. Çevrimiçi merak faktörü açısından incelendiğinde araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamında öğrenim gören kontrol grubu öğrencilerinin öntest ve sontest puanlarında anlamlı bir farklılığın olmadığı görülmektedir (t=-,785; p>,05). Kontrol grubunda yer alan öğrencilerin yarı deneysel işlem öncesi çevrimiçi merak faktörü öntest puanları ortalaması $\bar{X}$=36,65 iken, geleneksel yöntem ile eğitim gördükten sonra çevrimiçi merak faktörü puanları ortalaması $\bar{X}$=37,65'e yükselmiştir. Siber tehdit farkındalığı faktörü açısından incelendiğinde geleneksel yöntem ile öğrenim gören kontrol grubu öğrencilerinin öntest ve sontest puanlarında anlamlı bir farklılığın olmadığı görülmektedir (t=-1,244; p>,05). Kontrol grubunda yer alan öğrencilerin yarı deneysel işlem öncesi siber tehdit farkındalığı faktörü öntest puanları ortalaması $\bar{X}$=24,10 iken, geleneksel yöntem ile eğitim gördükten sonra çevrimiçi merak faktörü puanları ortalaması $\bar{X}$=25,25'e yükselmiştir. Bu bulgulara göre geleneksel yöntem ile yapılan öğretimin bilgi güvenliği farkındalık ölçeği ve alt faktörlerinin puanlarına etkisi olmasına rağmen anlamlı bir farklılığın olmadığı fakat bu konuda hali hazırda bilişim teknolojileri dersi kapsamında bilgi güvenliğine yönelik geleneksel ortamda verilen eğitimlerin öğrencilerinin bilgi güvenliği farkındalığına etkisi olduğu söylenebilir.

4.1.4. Deney ve Kontrol Grubu Öğrencilerinin Bilgi Güvenliği Farkındalık Ölçeği Öntest Puanları Kontrol Edildiğinde Sontest Bilgi Güvenliği Farkındalık Düzeyi Puanlarına İlişkin Bulgu ve Yorumlar

Araştırmanın üçüncü alt amacında ise iki ayrı ortamda öğrenim gören öğrencilerin başarılarında gözlenen söz konusu değişmelerin anlamlı bir farklılık gösterip göstermediğine ilişkin cevap aranmıştır. Öğrencilerin öğrenim gördüklerin ortamlara ait öntest-sontest puan ve standart sapma değerleri tablo 20'de sunulmuştur.

Tablo 20

Öğrencilerin ortaokul düzeyi bilgi güvenliği farkındalık ölçeği öntest puanları kontrol altına alındığında sontest puanlarına ait betimsel veriler

Grup	N	Sontest		Düzeltilmiş Sontest	
		$\bar{X}$	SS	$\bar{X}$	SH
Deney	20	139,5	8,88	137,86	2,92
Kontrol	20	123,65	17,90	125,28	2,92

Tablo 20 incelendiğinde deney grubunda yer alan öğrencilerin yarı deneysel işlem öncesi öntest puanları kontrol altına alındığında, sontest bilgi güvenliği farkındalık ortalama puanları $\bar{X}$=139,5, düzeltilmiş ortalaması ise $\bar{X}$=137,86'dır. Bunun yanında kontrol grubunda yer alan öğrencilerin yarı deneysel işlem öncesi öntest puanları kontrol altına alındığında, sontest bilgi güvenliği farkındalık ortalama puanları $\bar{X}$=123,65, düzeltilmiş ortalaması ise $\bar{X}$=125,28'dir. Bu doğrultuda, sontest bilgi güvenliği puanları arasında görülen bu farkın anlamlı olup olmadığını test etmek amacıyla kovaryans analizi (ANCOVA) yapılmıştır. Kovaryans analiz sonuçları Tablo 21'de sunulmuştur.

Tablo 21

Deney grubu ve kontrol grubu öğrencilerinin bilgi güvenliği farkındalık ölçeği öntest puanları kontrol edildiğinde, düzeltilmiş sontest puanlarına ait kovaryans analizi

Varyansın Kaynağı	Kareler Toplamı	Sd	Kareler ortalaması	F	p
Öntest	1474,119	1	1474,119	8,916	,005
Gruplama Ana Etkisi	**1477,018**	**1**	**1477,018**	**8,933**	**,005**
Hata	6117,431	37	165,336		
Toplam	702583	40			

Araştırmaya katılan deney ve kontrol grubu öğrencilerinin öntest bilgi güvenlik farkındalık düzeyi puanları kontrol altına alınıp, deney ve kontrol gruplarının düzetilmiş sontest bilgi güvenliği farkındalık düzeyi puanlarına ilişkin gruplama ana etkisinde anlamlı bir farklılığın olduğu belirlenmiştir ($F_{(1,37)}$: 8,93; p<,05). Bu bulguya göre araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamında öğrenim gören deney grubu öğrencilerin düzeltilmiş sontest bilgi güvenliği farkındalık düzeyi ortalama puanının

($\bar{X}$=137,86), öğrenme ortamını kullanmayan kontrol grubu öğrencilerinin ortalama puanlarına ($\bar{X}$=125,28) göre daha yüksek olduğu anlaşılmaktadır.

4.2. Nitel Verilere İlişkin Bulgu ve Yorumlar

Araştırmaya katılan görev temelli çevrimiçi öğrenme ortamında öğrenim gören öğrencilerin öğrenme ortamına ve öğrenme sürecine ilişkin görüşleri araştırmacı tarafından geliştirilen açık uçlu soru formuyla toplanmıştır. Deney grubunu oluşturan 20 öğrenciden elden edilen veriler içerik analiz yöntemiyle analiz edilmiştir. Böylelikle araştırmada elde edilen nitel bulgularla nicel bulguların desteklenmesi amaçlanmıştır.

4.2.1. Görev Temelli Çevrimiçi Öğrenme Ortamına İlişkin Bulgu ve Yorumlar

Araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamında öğrenim gören öğrencilerin öğrenme ortamına ilişkin görüşleri açık uçlu soru formuyla toplanmıştır. Bu doğrultuda elde edilen veriler içerik analiz yöntemiyle analiz edilerek içerik analizi sonucu ortaya çıkan alt temalar Tablo 22'de verilmiştir.

Tablo 22

Öğrencilerin görev temelli çevrimiçi öğrenme ortamına yönelik görüşleri

Olumlu	***f***	***%***
Ortamın İlgi Çekici Olması	14	70,0
Kullanım Kolaylığı	12	60,0
Yönergelerin Anlaşılabilir Olması	11	55,0
Olumsuz		
Teknik Sorunlar (hız, gecikme vb.)	5	25,0
İlgi Çekici Olmaması	2	10,0

Tablo 22'de görüldüğü üzere görev temelli çevrimiçi öğrenme ortamında öğrenim gören öğrencilerin birçoğunun öğrenme ortamına ilişkin görüşlerinin olumlu yönde olduğu belirlenmiştir. K7'in *"Güzel olan yani bir şeyleri öğrenirken eğlenceli hale gelmesi.*

Görevler çok zorlayıcı değildi benim açımdan. Rahatlıkla yapabildim.", K10'un *"Bilgilendirmeler çok faydalıydı, kullanımı çok kolaydı kolayca etkinlikleri gerçekleştirdim."* ve K5'in *"Öğrenme ortamının çok zarif olması ve istediğiniz şeyi anında bulabilmeniz olumlu yönleridir.* şeklinde ifade ettikleri üzere geliştirilen öğrenme ortamının ilgi çekiciliği ve kullanım kolaylığı öğrenciler tarafından vurgulanmaktadır. Bunun yanı sıra öğrenme ortamına ilişkin olumsuz görüş bildiren K5 *"Olumsuz bulduğum yanı giriş ekranı. Bazen bilgilerinizi doğruda yazsanız giremiyorsunuz siteye ama çok nadir oluyor."* ve K1'in *"Başlangıçta siteye şifremle giriş yapmakta zorlandım bundan dolayı öğretmenimden destek aldım."* Şeklindeki görüşleri geliştirilen öğrenme ortamında araştırmacının elinde olmayan sebepler doğrultusunda teknik sorunların olduğu ortaya çıktığı söylenebilir. Bu doğrultuda ADDIE bileşenleri ve görev temelli öğrenme yaklaşımına yönelik ilkeler göz önünde bulundurularak geliştirilmiş olan öğrenme ortamının öğrencilerin öğrenme ortamına yönelik görüşlerini olumlu yönde etkilediği söylenebilir.

4.2.2. Görev Temelli Çevrimiçi Öğrenme Ortamı Sürecine İlişkin Bulgu ve Yorumlar

Araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamında öğrenim gören öğrencilerin öğrenme sürecine ilişkin görüşleri açık uçlu soru formuyla toplanmıştır. Elde edilen veriler içerik analiz yöntemiyle analiz edilerek içerik analizi sonucu ortaya çıkan alt temalar Tablo 23'te verilmiştir.

Tablo 23

Öğrencilerin görev temelli çevrimiçi öğrenme ortamında öğrenme sürecine yönelik görüşleri

Olumlu	***f***	***%***
Görevler sonrası kazanılan rozetlerin motive edici olması	16	80,0
Diğer dersler için benzer ortamın kullanılma isteği	10	50,0
Verilen görevlerin ilgiyi arttırması	14	70,0
Olumsuz		
Görev zorluk seviyesi	6	30,0
Görev sayısının fazla olması	4	20,0

Tablo 23'te görüldüğü üzere görev temelli çevrimiçi öğrenme ortamında öğrenim gören öğrencilerin birçoğunun öğrenme sürecine ilişkin görüşlerinin olumlu yönde olduğunu belirlenmiştir. K5'in *"Kazandığım her Rozette daha çok görev yapasım geldi. Sertifika aldığımda ise keşke daha fazla görev olsa diyordum. Gerçekten motive ediyor."*, K9'un *"Web sitesinin en güzel yanının rozet ve sertifikalar olduğunu söyleyebilirim. Bu gibi durumların motive edici olduğunu ve bizleri teşvik ettiğini söyleyebilirim."* ve K2'in *"Evet görevler sonrası kazandığım rozetler beni çok sevindirdi, arkadaşlarıma kazandığım rozetleri gösterdim."* Şeklinde belirttikleri görüşler göz önünde bulundurulduğuna araştırmacı tarafından görevler sonrası verilen rozet ve sertifikaların öğrencileri olumlu yönde motive ve mutlu ettiği söylenebilir. Bunun yanı sıra, K13'ün *"Dersler bu şekilde olursa daha iyi öğrenebiliriz belki. Ama her ders için uygun olmayabilir. Mesela matematik için uygun olmayabilir çünkü matematik gibi derslerde birisinin size o an açıklamalı anlatması ve aklımıza takılan soruları hemen cevaplaması lazım."*, K16'nın *"Kullanılabilir. Hatta kullanılmalı da. Örnek verecek olursak; matematik, fen ve teknoloji, tarih derslerinde kullanılabilir. Benzer şekilde fen bilimleri dersinde maddenin halleri konusu işlenirken benzer karakter konunun olumlu olumsuz yönleriyle ilgili bilgilendirme yapabilir."* Ve K4'ün *"Matematik dersinde kullanılabilir. Her ünite için ayrı görevler verilebilir ve her üniteye ait bir sertifika kazanabiliriz."* Şeklinde belirttikleri görüşleri göz önünde bulundurulduğunda öğrencilerin geliştirilen öğrenme ortamını farklı derslerde de kullanmak istedikleri söylenebilir. Araştırmacı tarafından geliştirilen öğrenme ortamında öğrenim gören öğrencilerin sürece yönelik olumsuz olarak nitelendirdikleri en önemli unsurun görev zorluğuna yönelik olduğu görülmektedir. K6'nın *"Bazı görevler çok uğraştırıcıydı."* Ve K12'nin *"Görevlere biraz daha görsel ve etkileşimli içerikler eklenebilirdi. Açıkçası benim açımdan pek de zorlayıcı olmadı."* şeklinde görüşlerin göz önünde bulundurulduğunda sınırlı sayıda da olsa bazı öğrencilerin görevlerin zorluk seviyeleri hakkında olumsuz görüşleri bulunmaktadır. Tüm bu sonuçlar göz önünde bulundurulduğunda deney grubu öğrencilerinin büyük bir bölümünün öğrenme sürecine yönelik uygulama sürecinde verilen rozet ve sertifikaların motivasyonu arttırdığını ve görevlerin ilgi çekici olduğunu belirtmişlerdir. Bunun yanında deney grubu öğrencilerinin küçük bir bölümünün, görevlerin zorluk seviyesine yönelik olumsuz görüş bildirdikleri görülmüştür.

BEŞİNCİ BÖLÜM
TARTIŞMA, SONUÇ VE ÖNERİLER

Bu bölümde gerçekleştirilen uygulama sonuçlarının ana hatları özetlenmiş; elde edilen araştırma bulgulara dayalı olarak varılan sonuçlar mevcut literatürlerle tartışılarak verilmiştir. Ayrıca elde edilen sonuçlara göre ileride yapılacak çalışmalara yönelik önerilere yer verilmiştir.

5.1. Tartışma ve Sonuçlar

Bu araştırmada, ilköğretim düzeyi ortaokul kademesinde öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini arttırmaya yönelik görev temelli çevrimiçi öğrenme ortamının geliştirilmesi ve etkililiğinin belirlenmesi amaçlanmıştır. Bu amaç doğrultusunda çalışma, karma araştırma yöntemlerinden açıklayıcı sıralı desen ile tasarlanmıştır. Nicel ve nitel olmak üzere iki boyuttan oluşan çalışmanın nicel boyutunda öntest-sontest kontrol gruplu 2X2'lik bir split plot yarı deneysel desen kullanılmıştır. Araştırmanın nitel boyutunda ise Uygulama aşamasının nitel boyutunda ise öğrencilerin öğrencilerinin görev temelli çevrimiçi öğrenme ortamına ilişkin görüşleri açık uçlu soru formu kullanılmıştır. Bu bağlamda araştırma kapsamında nicel ve nitel verilere yönelik ulaşılan sonuçlar ile ilgili araştırmalar bağlamında bu sonuçlarla ilgili olarak yapılan tartışmalar ve öneriler aşağıda sunulmuştur.

5.1.1. Nicel Verilere Yönelik Sonuçlar

Araştırmanın nicel boyutunda olan öntest-sontest kontrol gruplu yarı deneysel desen sürecine geçmeden önce öğrencilerin bilgi güvenliği farkındalık düzeylerinin belirlenmesi yoluna gidilmiştir. Ancak çalışmanın amacı doğrultusunda bilgi güvenliği farkındalık düzeyini ölçmeye yönelik araştırma grubuna uygun bir ölçme aracı bulunamamış ve öncelikle ölçek geliştirme çalışması gerçekleştirilmiştir. Ölçek geliştirme süreci sonrasında ise araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamının ortaokul

öğrencilerinin bilgi güvenlik farkındalık düzeylerine etkisinin belirlemeye yönelik yarı deneysel sürece geçilmiştir.

Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeylerini belirlemek amacıyla araştırmacı tarafından "Ortaokul Düzeyi Bilgi Güvenliği Farkındalık Ölçeği" geliştirilmiştir. Ölçme aracının geliştirilmesi sürecinin AFA aşamasında 410 öğrencinin verisi değerlendirilmiş ve analizler sonucunda ölçme aracı yeniden düzenlenmiştir. Elde edilen yeni form ise çalışmanın DFA'sı için tekrar uygulanmış ve bu aşamada toplam 265 öğrenciden elde edilen veriler ile ölçeğin geçerlik ve güvenirlik çalışmaları yapılmıştır. Ölçek geliştirme çalışması sonucunda "çevrimiçi güvenlik farkındalığı", "çevrimiçi merak" ve "siber tehdit farkındalığı" olmak üzere üç faktör ve otuz maddeden oluşan ölçeğin Cronbach Alfa iç tutarlılık katsayısı ,90 olarak belirlenmiştir. Ölçeğin alt faktörlerinin belirlenmesi amacıyla gerçekleştirilen Cronbach Alfa iç tutarlılık analiz değerleri ise; çevrimiçi güvenirlik farkındalığı faktörü için ,94, çevrimiçi merak faktörü için ,90 ve siber tehdit farkındalığı faktörü için ,86 olarak ortaya çıkmıştır. Buna göre faktörlerin Cronbach Alfa iç tutarlılık katsayısı ,70'ten yüksek olduğu tespitinde yola çıkarak ölçeğin güvenilir ve tutarlı bir ölçek olduğu sonucuna ulaşılmıştır (Nunnally, 1978; Tavşancıl, 2005).

Ölçek geliştirme süreci sonrasında ise nitel ve nicel verilerin işe koşulduğu karma araştırma yöntemlerinden açıklayıcı sıralı desenin benimsendiği çalışmanın uygulama aşamasına geçilmiştir. Öğrencilerin bilgi güvenliği farkındalığının sağlanmasına yönelik çevrimiçi görev temelli ortamın etkisinin belirlenmesini tespit etmek için çalışmanın nicel boyutunda öntest-sontest kontrol gruplu 2X2'lik bir split plot yarı deneysel desen kullanılmıştır. Bu aşamada öncelikle ADDIE modeli bileşenleri ve uzman görüşlerine dayalı olarak deneysel ortam(çevrimiçi görev temelli ortam) hazırlanmıştır. Bu süreç içerisinde ayrıca görev temelli çevrimiçi öğrenme ortamına uygun olarak uzman görüşleri doğrultusunda bilgi güvenliği kazanımlarına yönelik görevler geliştirilmiştir. Araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamının bilgi güvenliği farkındalık düzeyine etkisini belirlemek amacıyla ilköğretim düzeyi ortaokul kademesinde öğrenim gören 20 deney grubu, 20 kontrol grubu olmak üzere toplam 40 öğrenci üzerinde 5 hafta süren uygulama yapılmıştır. Bu doğrultuda araştırmacı tarafından geliştirilen ortaokul düzeyi bilgi güvenliği farkındalığı ölçeği, deney ve kontrol gruplarına uygulama öncesinde

öntest, sonrasında ise sontest olarak uygulanmıştır. Araştırma öncesi çalışmanın gerçekleştirildiği sınıflar arasında homojenliğin sağlandığı ve dağılımın normallik varsayımını yerine getirmesinden dolayı tüm gurubun çalışma için ön gereksinimleri yerine getirdikleri belirlenmiş ve parametrik yöntemlerle analizleri gerçekleştirilmiştir.

Gerçekleştirilen analizler sonucunda deney ve kontrol grubunun öntest bilgi güvenliği farkındalık düzeyi puanları arasında istatistiksel olarak anlamlı bir farklılık olmadığı görülmüştür. Bu sonuç grupların uygulama öncesinde bilgi güvenliği farkındalık düzeylerinin benzer olduğunu göstermektedir. Bu analiz sonucunda çalışma gerçekleştirilmiş ve çalışma sonucunda yapılan sontest sonrasında deney ve kontrol grubu öğrencilerinin sontest bilgi güvenliği farkındalık düzeyi puanları arasında anlamlı bir farklılığın olduğu sonucuna ulaşılmıştır. Bu sonuca göre araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamının öğrencilerin bilgi güvenliği farkındalık düzeyine olumlu bir etkisi olduğu görülmektedir. Konuyla ilgili Serter (2021), ortaokul öğrencilerinin bilgi güvenliği farkındalığına ilişkin yaptığı çalışmada öğrencilerin internete ayırdıkları günlük süre ile bilgi güvenliği farkındalığı ortalama puanları arasında anlamlı bir farklılığın olmadığını belirtmiştir. Wu vd., (2021) bilgi güvenliği eğitiminin öğrencilerinin bilgi güvenliği farkındalığı geliştirmek için etkili bir yöntem olduğunu savunarak yaptığı çalışma sonucunda oyunlaştırılmış sınıftaki öğrencilerin geleneksel yöntem ile eğitim alan öğrencilerden bilgi güvenliği davranışı konusunda daha iyi performans ortaya koyduğu ve öğrenme ortamının bilgi güvenliği farkındalığını arttırma üzerinde cinsiyet arasında fark gözlemlenmemiştir. Mıhçı vd., (2019), yaptıkları çalışmada öğrencilerin siber zorbalık, internet bağımlığı ve çevrimiçi güvenlik anlamında farkındalıklarının yüksek olduğunu ancak uygunsuz içerik ve telif hakkı konusunda ise farkındalıklarının orta seviyede olduğunu belirtmiştir. Smahel vd., (2020), 19 ülkeden 7-17 yaş aralığındaki internet kullanıcısının katılım gösterdiği Avrupa Çevrimiçi Çocuk (EU Kids Online) projesinde, internet kullanıcılarının birçok çevirimiçi projeye katılım göstermesinin sebebinin çevrimiçi ortamda kendilerini güvende hissetmek olduğunu belirtmiştir.

Deney grubu öğrencileri üzerinde gerçekleştirilen analiz sonucunda deney grubu öğrencilerinin bilgi güvenlik farkındalık ölçeği ve alt faktör öntest ve sontest bilgi güvenliği farkındalık düzeyi puanları arasında anlamlı bir farklılığın olduğu sonucuna varılmıştır. Bu

sonuca göre araştırmacı tarafından geliştirilen öğrenme ortamının bilgi güvenliği farkındalık ölçeği ve alt faktörlerinin bilgi güvenliği farkındalık düzeyi puanlarını arttırma konusunda önemli bir etkiye sahip olduğu söylenebilir. Zolotarev vd., (2021) lisans son sınıf ve bilgi güvenliği yüksek lisans son sınıf öğrencileri üzerinde bilgi güvenliği farkındalığını arttırmak için geliştirdikleri ortamın olumlu yönde etkisi olduğu belirtmişlerdir. Tekerek ve Tekerek (2013), ortaöğretim öğrencileri üzerinde gerçekleştirdikleri çalışmada bilgi güvenlik farkındalık düzeylerinin yeterli seviyede olduğu belirtmiştir. Hacımustafaoğlu (2019), yaptığı çalışmada ortaöğretim öğrencilerinin bilgi güvenlik farkındalık düzeyinin orta seviyede olduğunu belirtmiş ve öğrencilerin kişisel verilerini ve mahremiyetini önemsediklerini ve önlem aldıklarını ileri sürmüştür. Akyüz (2012), geliştirdiği görev temelli öğrenme ortamının öğrencilerinin motivasyonunu artırdığını belirtmiş ve öğrenme ortamının öğrencilerin problem çözme becerileri üzerinde anlamlı bir etkiye sahip olduğunu tespit etmiştir. Kontrol grubu öğrencileri üzerinde gerçekleştirilen analiz sonucunda kontrol grubu öğrencilerinin bilgi güvenlik farkındalık ölçeği ve alt faktör öntest ve sontest bilgi güvenliği farkındalık düzeyi puanları arasında anlamlı bir farklılığın olmadığı sonucuna varılmıştır. Bu sonuca göre geleneksel yöntem ile yapılan öğretimin bilgi güvenliği farkındalık ölçeği ve alt faktörlerinin puanlarına etkisi olmasına rağmen anlamlı bir farklılığın olmadığı fakat bu konuda hali hazırda bilişim teknolojileri dersi kapsamında bilgi güvenliğine yönelik geleneksel ortamda verilen eğitimlerin öğrencilerinin bilgi güvenliği farkındalığına etkisi olduğu söylenebilir. Gökmen ve Akgün (2015), lisans öğrencileri üzerinde gerçekleştirdiği çalışmada öğrencilerin bilgi güvenliği farkındalık düzeylerinin düşük olduğunu belirtmiştir. Yılmaz vd., (2017), liselerde öğrenim gören öğrenciler üzerinde yaptıkları araştırmada öğrencilerin bilgisayar ve internet kullanımı farkındalığının çok az sayıda kişide yüksek olarak belirtmiştir. Genç (2021), bilgi toplumu ve dijital dönüşüm kavramları çerçevesinde bireylerin bilgi güvenliği açısından bilişim teknolojileri ve internet kullanımlarına yönelik davranışları üzerine gerçekleştirdiği çalışmada kişilerin kullanım, alışkanlık, davranış ve bilgi güvenliği farkındalığı açısından farklı özellikler gösterdiğini ortaya koymuştur.

Deney ve kontrol grubu öğrencileri üzerinde gerçekleştirilen öntest bilgi güvenlik farkındalık düzeyi puanları kontrol altına alındığında, deney ve kontrol gruplarının düzetilmiş sontest bilgi güvenliği farkındalık düzeyi puanlarına ilişkin analizler sonucunda

da gruplama ana etkisinin anlamlı bir farklılığın olduğu sonucuna ulaşılmıştır. Bu sonuca göre araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamında öğrenim gören deney grubu öğrencilerin düzeltilmiş sontest bilgi güvenliği farkındalık düzeyi puanının, öğrenme ortamını kullanmayan kontrol grubu öğrencilerinin puanlarına göre daha yüksek olduğu anlaşılmaktadır. Bir başka deyişle görev temelli çevrimiçi öğrenme ortamının öğrencilerinin bilgi güvenliği farkındalık düzeylerini artırmada etkili bir ortam olduğu ve hazırlanan görevlerin etkili görevler olduğu görülmektedir. Sarı (2021), yaptığı çalışmada, ortaokul öğrencilerinin çevrimiçi güvenlik ve risk ile ilgili eğitimlerine dair çevrimiçi bir ortam tasarlayarak gerçekleştirdiği çalışmada öğrencilerin sanal ortamlarda bilgi güvenliğine ilişkin öğrenmelerinin tasarlanan ortamdaki eğitimler sonrasında yükseldiği sonucuna ulaşmıştır. Güldüren (2015), öğretim elemanlarının geliştirilen çoklu ortam materyalleri ve web sitesi kullanımı sonrası bilgi güvenliği farkındalığı puanlarında artış olduğunu belirtmiştir. Teker (2019), lise öğrencileri ve öğretmenler üzerinde gerçekleştirdiği çalışma sonucunda öğretmenlerin bilgi güvenliği farkındalık düzeylerinin bilgisayar kullanma ile ilgili aldıkları eğitim ve bu eğitimi yeterli bulma durumlarına göre anlamlı bir farklılık bulurken cinsiyetlerine ve meslekteki hizmet sürelerine göre anlamlı bir farklılığın olmadığını tespit etmiştir. Bununla birlikte, lise öğrencilerinin bilgi güvenliği farkındalık düzeylerinin ise cinsiyetlerine, eğitim gördükleri okul türlerine, ve bilgisayar kullanma ile ilgili aldıkları eğitime göre anlamlı bir farklılık bulurken, yaş ve sınıf değişkenlerine göre anlamlı bir farklılığın olmadığını tespit etmiştir. Metli (2017), 309 ortaokul öğrencisi üzerinde gerçekleştirdiği çalışmada kişisel bilgisayara sahip olan öğrencilerin siber mağduriyetlerinin kişisel bilgisayara sahip olmayan öğrencilerden daha fazla olduğunu belirtmiştir. Kaşıkçı vd., (2016), tarafından gerçekleştirilen çalışmada günümüz öğrencilerinin günlük internet kullanım ortalamalarının yüksek olmasına rağmen internet okuryazarlığı ile ilgili farkındalıklarının düşük olduğu belirtilmiştir. Akgün ve Topal (2015), bilgisayar kullanma tecrübesinin arttıkça bilgi güvenliği farkındalığının arttığını fakat bu artış ile birlikte etik dışı kullanımın da arttığını ifade etmiştir. Baran ve Şener (2019), yeterli fiziki koşulların oluşturularak, yasal sorumluluklar çerçevesinde uzman kişiler aracılığıyla bilgi güvenliğinin oluşturulmasını gerektiğini ve personellerin bu konuda eğitime ihtiyacı olduğunu belirtmişlerdir.

5.1.2. Nitel Verilere Yönelik Sonuçlar

Deney grubu öğrencilerinin görev temelli çevrimiçi öğrenme ortamına yönelik görüşleri incelendiğinde, geliştirilen öğrenme ortamının ilgi çekici olduğu, ortamda bulunan yönergelerin anlaşılır şekilde sunulduğu ve kullanım açısından kullanıcı dostu olduğu öğrenciler tarafından vurgulanmıştır. Bunun yanında öğrencilerin küçük bir bölümünün araştırmacının elinde olmayan teknik sebeplerden kaynaklı sorunlar yaşadıkları görülmüştür. Bununla birlikte öğrencilerin görev temelli çevrimiçi öğrenme sürecine yönelik görüşleri incelendiğinde ise, öğrencilerin büyük bir bölümünün olumlu cevaplar verdikleri görülmüştür. Araştırmacı tarafından görevler sonrası verilen ödüllerin (rozet ve sertifikalar) öğrencileri olumlu yönde motivasyonu arttırdığı ve aynı zamanda öğrencilerin geliştirilen öğrenme ortamını farklı derslerde de kullanmak istedikleri görülmüştür. Bunun yanında öğrencilerin küçük bir bölümünün görevlerin zorluk seviyesine yönelik olumsuz görüş belirttikleri tespit edilmiştir. Ahlan vd., (2015), kullanıcı bakış açısına dayalı eğitim programı stratejisi oluşturmanın, yükseköğretim düzeyinde bilgi güvenliği farkındalığının artmasında önemli rol oynadığını belirtmişlerdir. Tam vd., (2022) kurumların, bilgi güvenliği politikalarını uymaları için çalışanları motive etmek, mutlu etmek ve memnun tutmak gibi şirketlerin düşük maliyetli önlemler ile çalışanların bilgi güvenliği farkındalıklarının olumlu yönde etkilendiğini belirtmişlerdir. Sharma ve Aparicio (2022) organizasyon kültürü ve ekip kültürü faktörlerinin, çalışanların algılanan bilgi güvenliği tehditleri ve bilgi güvenliği politikalarına uyumuna yönelik motivasyonları üzerindeki etkisi üzerinde gerçekleştirdiği çalışmada, hem organizasyon hem de ekip kültürünün, çalışanların bilgi güvenliği tehditlerini değerlendirme ve başa çıkma algılarını etkilediğini ve bu doğrultuda bilgi güvenliği politikalarına uymaya yönelik davranışsal niyetinide olumlu etkilediğini belirtmişlerdir. Tüm bu sonuçlar göz önünde bulundurularak araştırmacı tarafından geliştirilen görev temelli çevrimiçi öğrenme ortamının öğrencilerin bilgi güvenliği bilgi güvenliğine farkındalıklarına yönelik etkisine yönelik araştırma sorusunun karşılandığı görülmektedir. Bu anlamda genel olarak bilgi güvenliğine yönelik eğitimlerin ilköğretim düzeyinden başlayarak çevrimiçi ortamlarla ve çoklu ortam materyalleriyle verilerek bilgi güvenlik farkındalıklarının kazandırılması önem arz etmektedir.

5.2. Öneriler

Bu bölümde, araştırma sonucu elde edilen araştırma bulgularına dayalı olarak uygulamaya ve ileride yapılacak araştırmalara yönelik önerilere yer verilmiştir.

5.2.1. Uygulamaya Yönelik Öneriler

- Çalışmada elde edilen veriler doğrultusunda görev temelli çevrimiçi öğrenme ortamı aracılığı ile bilgi güvenliği farkındalığının arttırılabildiği belirlenmiştir. Bu doğrultuda geliştirilen öğrenme ortamı ve uygulanan stratejiler göz önünde bulundurularak tüm öğrencileri kapsayacak nitelikte tasarımlar işe koşulmalıdır.
- Bilgi güvenliği farkındalığına yönelik görevlerin zorluk düzeyleri üzerinde yeni tasarımlar gerçekleştirilebilir.
- Geliştirilen öğrenme ortamında kullanılacak olan içerikler ses, görsel, video olarak çeşitlendirilebilir.
- Rekabet ve ödül sisteminin öğrencileri olumlu yönde etkilediği görülmüştür. Bu noktada çalışmalarda farklı ödül sistemleri kullanılarak öğrenci motivasyonu arttırılabilir.

5.2.1. İlerde Yapılabilecek Araştırmalara Yönelik Öneriler

- Geliştirilen öğrenme ortamının farklı konularda uygulanması bu yaklaşımının farklı alanlarda da öğrenci üzerindeki etkisinin incelenmesi sağlanabilir.
- Bu araştırma ilköğretim düzeyi ortaokul kademesinde öğrenim gören öğrenciler üzerinde gerçekleştirilmiştir. Bu çalışmanın benzeri farklı hedef kitleler üzerinde gerçekleştirilebilir.
- Bilgi güvenliği farkındalığı konusunu siber zorbalık, siber mağduriyet, dijital vatandaşlık ve dijital ayak izi gibi farklı konular bir arada olacak şekilde farklı çalışmalar gerçekleştirilebilir.

KAYNAKÇA

Abaido, G. M. (2020). Cyberbullying on social media platforms among university students in the United Arab Emirates. *International Journal of Adolescence and Youth, 25*(1), 407-420.

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

Abdillah, R., Shukur, Z., Mohd, M. and Murah, M. Z. (2022). Phishing Classification Techniques: A Systematic Literature Review. *IEEE Access. 10*, 41574–41591.

Acılar, A. (2009). İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi, 1*(1), 25-33.

Ahlan, A. R., Lubis, M. and Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: its antecedents and measures. *Procedia Computer Science, 72,* 361-373.

Akgün, Ö.E. ve Topal, M. (2015). Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği. *Sakarya University Journal of Education*, 5(2), 98-121.

Akyüz, H. İ. (2012). *Çevrimiçi görev temelli öğrenme ortamında eğitsel ajanın rolünün ve biçim özelliklerinin öğrencilerin motivasyonuna, bilişsel yüklenmesine ve problem çözme becerisi algısına etkisi*. (Kayıt No. 311765) [Doktora Tezi. Ankara Üniversitesi]. YÖK Tez Merkezi.

Alhogail, A. (2015) Design and Validation of Information Security Culture Framework. *Computers in Human Behavior, 49*, 567-575.

AlKalbani, A., Deng, H. and Kam, B. (2015). *Organisational security culture and information security compliance for e-government development: the moderating effect of social pressure*. Pacis2015, 65.

Allen, W. (2006). Overview and evolution of the ADDIE training system. *Advances in Developing Human Resources, 8*, 430-441.

Allers, J., Drevin, G. R., Snyman, D. P., Kruger, H. A. and Drevin, L. (2021). Children's Awareness of Digital Wellness: A Serious Games Approach. *In IFIP World Conference on Information Security Education, 615*, 95-110.

Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg and E. Almomani. (2013). A Survey of Phishing Email Filtering Techniques. *IEEECommunications Surveys Tutorials 15*, (4), 2070–2090.

Arce, I. (2003). The weakest link revisited [information security]. *IEEE Security & Privacy, 1*(2), 72-76.

Atkinson, S., Furnell, S. and Phippen, A. (2009). Securing The Next Generation: Enhancing E-Safety Awareness Among Young People. *Computer Fraud & Security, 7*, 13-19.

Bada, M., Sasse, A. M. and Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *In: International Conference on Cyber Security for Sustainable Society*, 118–131.

Balcı, A. (2009). *Sosyal bilimlerde araştırma yöntem, teknik ve ilkeler. (7.b.).* Ankara: Pegem Akademi.

Banerjee, C., Banerjee, A. and Murarka, P. D. (2013). An Improvised Software Security Awareness Model, *International Journal of Information, Communication & Computing Technology, 1*(2), 43–48.

Baran, S. ve Şener, E. (2019). Hastanelerde Bilgi Güvenliği Yönetimi: Nitel Bir Araştırma. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, *10*(23), 108-125.

Başaran, B. (2010). *Web Tabanlı Sistemlerde Scorm Uyumlu Whiteboard Movie Tekniğinin Öğrencilerin Fizik Derslerindeki Başarı ve Tutumlarına Etkisinin Araştırılması* (Kayıt No. 275405) [Doktora Tezi, Dicle Üniversitesi]. YÖK Tez Merkezi.

Bensghir, T. K. (1996); *Bilgi Teknolojileri ve Örgütsel Değişim*, TODAİE Yayını, Ankara.

Bintziou, A., Alexandris, N. and Chrissikopoulos, V. (1999). Introducing IT-security Awareness in schools: the Greek Case. *In IFIP WG 11.8 1st World Conference on Information Security Education WISE1*.

Blackley, J. A., Peltier, T. R. and Peltier, J. (2004). *Information security fundamentals*. Auerbach Publications. 1, 280.

Blanding, F. S. (2004). *An Introduction to LAN/WAN Security, Information Security Management Handbook*, Fifth Edition, Auerbach Publications, New York.

Brady, C. (2010). *Security Awareness for Children*. Technical Report RHUL–MA–2010–05 Department of Mathematics Royal Holloway, University of London Egham, Surrey TW20 0EX, England.

Branch, R. M. (2016). *Öğretim tasarımı: ADDIE yaklaşımı*. Eğitim Yayınevi.

Brown, J. S., Collins, A and Duguid, P (1989). Stuated Cognition and The Culture of Learning. *Educational researcher*, *18(*1), 32-42.

BTK. (2022). İnternet Kullanımında Çocuk ve Aile İlişkisi. Erişim adresi: https://internet.btk.gov.tr/internet-kullaniminda-cocuk-ve-aile-iliskisi

Büyüköztürk, Ş. (2002). Faktör Analizi: Temel Kavramlar ve Ölçek Geliştirmede Kullanımı. *Kuram ve Uygulamada Eğitim Yönetimi, 32*, 470-483.

Büyüköztürk, Ş. (2005). Anket geliştirme. *Türk Eğitim Bilimleri Dergisi*, 133-151.

Büyüköztürk, Ş. (2006). *Sosyal Bilimler İçin Veri Analizi El Kitabı. İstatistik, Araştırma Deseni SPSS Uygulamaları ve Yorum (6. Baskı).* Ankara: Pegem A yayıncılık.

Büyüköztürk, Ş., Çakmak, E. K., Akgün, Ö. E., Karadeniz, Ş. ve Demirel, F. (2016). *Bilimsel araştırma yöntemleri*. Ankara: Pegem Akademi.

Can, Ö. ve Akbaş, M., F. (2014). Kuramsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması. *TÜBAV Bilim Dergisi, 7*(2), 16-31.

Canbek, G., ve Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi, 9*(3), 165-174.

Chandarman, R. and Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educationalinstitution. *African Journal of Information and Communication, 20,* 133–155.

Chang, H. H., Wong, K. H. and Lee, H. C. (2022). Peer privacy protection motivation and action on social networking sites: Privacy self-efficacy and information security as moderators. *Electronic Commerce Research and Applications, 54,* 101176.

Cherdantseva, Y. and Hilton, J. (2013). A reference model of information assurance and security. 2013 *International Conference on Availability, Reliability and Security, Regensburg*, 546-555.

Cheung, L. (2016). Using the ADDIE model of instructional design to teach chest radiograph interpretation. *Journal of Biomedical Education*, 1-6.

Chou, H. L. and Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior, 65,* 334-345.

Clark, L. A. and Watson, D. (2019). Constructing validity: New developments in creating objective measuring instruments. *Psychological assessment, 31*(12), 1412.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days?. *Information security technical report, 14*(4), 186-196.

Corbin, J. M., and Strauss, A. C. (2007). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Thousand Oaks, CA: Sage Publication.

Creswell, J. W. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches. (2th ed.).* Thousand Oaks, CA: Sage.

Creswell, J. W. (2005). *Educational research: planning, conducting, and evaluating quantitative and qualitative research (2nd ed.)*. New Jersey: Merrill Prentice Hall.

Creswell, J. W. (2017). *Nitel Araştırmacılar için 30 Temel Beceri.* (çev. Hasan Özcan). Anı Yayıncılık, Ankara.

Creswell, J. W. and Plano Clark, V. L. (2007). *Designing and conducting mixed methods research.* Thousand Oaks, CA: Sage.

Curlette, W. (2006). A framework for research studies: Mixed methods through combining Bayesian statistics and qualitative research in individual psychology. *The Journal of Individual Psychology, 62*(3), 338-349.

Cüceloğlu, D. (2015). *İnsan ve Davranışı*. İstanbul: Remzi Kitapevi.

Çakır, H. (2006). Bir iletişim dili olarak internet. *Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 1*(19), 71-96.

Çakır, S. ve Kesler, M. (2012). Bilgisayar güvenliğini tehdit eden virüsler ve antivirüs yazılımları. *XIV. Akademik Bilişim Konferansı Bildirileri, 551*, 558.

Çakmak, E. K., Çebi, A. ve Kan, A. (2014). E-öğrenme ortamlarına yönelik sosyal bulunuşluk ölçeği geliştirme çalışması. *Kuram ve Uygulamada Eğitim Bilimleri, 14(2*), 755-768.

Çavusoglu, H., Raghunathan, S. and Çavusoglu, H. (2009). Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems. *Information Systems Research, 20*(2), 198-217.

Çek, E. (2017). *Kurumsal Bilgi Güvenliği Yönetişimi ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi* (Kayıt No. 496021) [Yüksek Lisans Tezi. İstanbul Bilgi Üniversitesi]. YÖK Tez Merkezi.

Çelen, F. K., Çelik, A. ve Seferoğlu, S. S. (2011). *Çocukların İnternet kullanımları ve onları bekleyen çevrim-içi riskler.* XIII. Akademik Bilişim Konferansı (AB11), 2-4 Şubat 2011, İnönü Üniversitesi, Malatya.

Çokluk, Ö., Şekercioğlu, G. ve Büyüköztürk, Ş. (2010). *Sosyal bilimler için çok değişkenli istatistik SPSS ve LISREL uygulamaları.* Ankara: Pegem Akademi.

Çolak, M. (2005). *Kütahya İli İlköğretim Okullarında Ödül ve Ceza* (Kayıt No. 187877) [Yüksek Lisans Tezi, Manisa Celal Bayar Üniversitesi]. YÖK Tez Merkezi.

Daalen, O. (2022). In defense of offense: information security research under the right to science. *Computer Law & Security Review, 46*, 105706.

DeGroot III, H., Uzunishvili, S., Weir, R., Al-omari, A. and Gomes, B. (2012). Intra-articular injection of hyaluronic acid is not superior to saline solution injection for ankle arthritis: a randomized, double-blind, placebo-controlled study. *J Bone Joint Surg Am*, *94*(1), 2-8.

DeVellis, R. F. (2014). *Ölçek geliştirme, kuram ve uygulamalar* (Çev. Ed. Tarık Totan). Ankara: Nobel.

DeVellis, R. F. and Thorpe, C. T. (2021). *Scale development: Theory and applications*. Sage publications.

Dhillon, G. (2017). *Information Security-Text & Cases (2nd ed.)*, Prospect Press, Burlington,

Dura, C. ve Atik H. (2002). *Bilgi Toplumu, Bilgi Ekonomisi ve Türkiye*, İstanbul: Literatür Yayıncılık.

Ellis, R. (2003), *Task-based language learning and teaching*. Oxford: Oxford University Press.

Eminağaoğlu, M. ve Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir, Türkiye' de bilgi güvenliği sorunları ve çözüm önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *11*(4), 1-15.

ENISA. (2019). *ENISA threat landscape report 2018: 15 Top Cyber-Threats and Trends.* Heraklion: european Network and Information Security Agency (ENISA).

Erol, S. E. ve Sağıroğlu, Ş. (2018). *Siber güvenlik farkındalığı, farkındalık ölçüm yöntem ve modelleri.* Şeref Sağıroğlu ve Mustafa Alkan (Ed.), Siber Güvenlik ve Savunma, Farkındalık ve Caydırıcılık içinde (21-45). Ankara: Grafiker Yayınları.

Esteves, J., Ramalho, E. and De Haro, G. (2017). To improve cybersecurity, think like a hacker. *MIT Sloan Management Review*, *58*(3), 71.

etinkaya, L. (2017). The Impact of Whatsapp Use on Success in Education Process. *The International Review of Research in Open and Distributed Learning*, *18*(7), 59-74.

Fortinet. (2022). What Are Computer Viruses? Erişim adresi: https://www.fortinet.com/resources/cyberglossary/computer-virus

Fraenkel, J. R. and Wallen, N. E. (2011*). How to design and evaluate research in education (8th ed.).* NY: McGraw-Hill Higher Education.

Gao, X., Gong, S., Wang, Y., Wang, X. And Qiu, M., (2022). An Economic Analysis of Information Security Decisions with Mandatory Security Standards in Resource Sharing Environments. *Expert Systems with Applications*, *206*, 117894.

Gawlik-Kobylińska, M. (2017). Task-based approach in 3d education for security and safety. *IJIT Security*, *9*(20), 3-12.

Geekforgeeks. (2022). What is Phishing? Erişim adresi: https://www.geeksforgeeks.org/what-is-phishing/

Gencer, K. (2015). *ISO 27001 kapsamında kurumsal bilgi güvenliğine dinamik bir yaklaşım* (Kayıt No. 398539) [Yüksek Lisans Tezi. Afyon Kocatepe Üniversitesi]. YÖK Tez Merkezi.

Genç, C. (2019). *Kişisel verilerin korunması kapsamında bilgi güvenliği farkındalığı analizi ve e-devlet yapısının incelenmesi* (Kayıt No. 584130) [Yüksek Lisans Tezi. İstanbul Okan Üniversitesi]. YÖK Tez Merkezi.

Geray, C. (2002). *Halk eğitimi*. Ankara: İmaj

González-Lloret, M. (2017). Technology for task-based language teaching. *The handbook of technology and second language teaching and learning, 1,* 234-247.

Gökmen, Ö. F. ve Akgün, Ö. E. (2015). Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Bilgilerinin Çeşitli Değişkenlere Göre İncelenmesi. *Çukurova Üniversitesi Eğitim Fakültesi Dergisi*, *44*(1), 61-84.

Green, J. C., Krayder, H. and Mayer, E. (2005). Combining qualitative and quantitative methods in social inquiry. In B. Somekh & C. Lewin (Eds.). *Research methods in the social sciences* (pp. 275-282). London: Sage

Gupta, B. B., Arachchilage, N. A. and Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247-267.

Güçdemir, Y. (2003). Bilgisayar ağları internetin gelişimi ve bilgi kirlenmesi. *İstanbul Üniversitesi İletişim Fakültesi Dergisi*, *17*, 371-378.

Güldüren, C. (2015). *Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi* (Kayıt No. 396156) [Doktora Tezi, Ankara Üniversitesi]. YÖK Tez Merkezi.

Güldüren, C., Çetinkaya, L. ve Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *İlköğretim Online 15*(2),682-695.

Gülmüş, M. (2010). *Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği* (Kayıt No. 295662) [Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi]. YÖK Tez Merkezi.

Hacımustafaoğlu, R. (2019). *Ortaöğretim öğrencilerinin bilgi güvenliği farkındalık düzeylerinin Siber mağdur olma durumlarına etkisinin incelenmesi (Üsküdar örneği)*. (Kayıt No. 586385) [Yüksek Lisans Tezi. Sakarya Üniversitesi]. YÖK Tez Merkezi.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7),

Haeussinger, F. and Kranz, J. (2017). Antecedents Of Employees'ınformatıon Securıty Awareness-Revıew, Synthesıs, And Dırectıons For Future Research. In *European Conference on Information Systems*. 1-20.

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

Harden, R. M., Laidlaw, J. M., Ker, J. S. and Mitchell, H. E. (1996). Task Based Learning: An Educational strategy For Undergraduate, Postgraduate and Continuing Medical Education, Part I. *Medical Teacher*, *18*(1), 1-7.

Haufe, K., Brandis, K., Colomo-Palacios, R., Stantchev, V. and Dzombeta, S. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management, 4*(4), 27–47

Hekim, H. ve Başıbüyük O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, *4*(2), 135-158

Helokunnas, T. and Kuusisto, R. (2003) "*Information Security Culture in a Value Net*", IEMC '03. Managing Technologically Driven Organizations: The Human Side of Innovation and Change.

Herath, A., Al-Bastaki, Y. and Herath, S. (2013). Task based Interdisciplinary E-Commerce Course with UML Sequence Diagrams, Algorithm Transformations and Spatial

Circuits to Boost Learning Information Security Concepts. *International Journal of Computing and Digital Systems*, *2*(02).

Horne, C.A., Ahmad, A. and Maynard, S.B. (2016). "A Theory on Information Security," *The 27th AustralasianConference on Information Systems*, Wollongong, Australia.

Hu, X., Tang, J., Zhang, Y. and Liu, H. (2013). Social spammer detection in microblogging. In *Twenty-third international joint conference on artificial intelligence*. 2633-2639.

Humaidi, N. and Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, *5*(4), 311.

Imgraben, J., Engelbrecht, A. and Choo, K. K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, *33*(12), 1347-1360.

Internet Live Stats. (2019). Internet live stats. https://www.internetlivestats.com/ adresinden 08.06.2022 tarihinde erişilmiştir.

ISO. (2022). International Organization for Standardization. Erişim adresi: http://www.iso.org/iso/en/stdsdevelopment/tc/tcli

Jaeger, L. (2018). *Information security awareness: Literature review and integrative framework.* In proceedings of the 51st Hawaii International Conference on System Sciences, 4703-4712.

Jain, A. K. and Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), 527-565.

Jansson, K. and von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & information technology*, *32*(6), 584-593.

Johnson, B. and Christensen, L. (2008). *Educational research: quantitative, qualitative and mixed approaches (3nd ed.)*. California: Sage.

Jöreskog, K. G. and Sörbom, D. (1993). *LISREL 8: Structural equation modeling with the SIMPLIS command language.* Scientific Software International; Lawrence Erlbaum Associates, Inc.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A. and Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & security, 43*, 64-76.

Kaminski, J. (2007). *Use ADDIE to Design Online Courses,* Nursing-informatics.com

Kang, M., Hovav, A., Lee, E. T., Um, S. and Kim, H. (2022). Development of methods for identifying an appropriate benchmarking peer to establish information security policy. *Expert Systems with Applications, 201*, 117028.

Karaahmetoğlu, G. (2021). Ortaokul Öğrencilerinin Bilgisayar Kullanımı ve İnternet Bağımlılığı Düzeylerinin İncelenmesi. *Erciyes Üniversitesi Sağlık Bilimleri Fakültesi Dergisi*, *7*(2), 1-9.

Karasar, N. (2005). *Bilimsel araştırma yöntemi kavramlar ilkeler teknikler*. Ankara: Nobel Yayınları.

Kaspersky. (2022). *What is Spyware?*. https://www.kaspersky.com/resource-center/threats/spyware adresinden 08.06.2022 tarihinde erişilmiştir.

Kass, R. A. and Tinsley, H. E. A. (1979). Factor analysis. *Journal of Leisure Research, 11*, 120-138.

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

Keser, H. ve Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *K.Ü. Kastamonu Eğitim Dergisi, 23*(3), 1167-1184.

Kesmez, N. (2002). *Kişisel Verilerin Korunması Kanunu (Taslak)*, Türkiye Bilişim Şurası, 2002,

Khando, K., Gao, S., Islam, S. M. and Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267.

Kılıç Aksu P., Çatar Ö., Şişman Kitapçı N., Köksal L. ve Mumcu G. (2015). *Hastane Bilgi Yönetim Sisteminde Bilgi Güvenliğinin Sağlık Çalışanları Tarafından Değerlendirilmesi,* Kişisel Sağlık Verileri Ulusal Kongresi, İstanbul.

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

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*. *22*(1), 115-126.

Kline, P. (1994). *An easy guide to factor analysis.* New York: Routledge.

Kline, P. (2000). *The Handbook of Psychological Testing* (2nd Edition). London and Newyork: Routledge.

Kline, P. (2005). *Principles and Practice of Structural Equation Modeling* (2nd ed.). New York: Guilford.

Koohang, A., Anderson, J., Nord, J. H. and Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems, 120*(1), 231- 247.

Korkmaz, İ. (2017). "*Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*", Seçkin yayınları, 74.

Kritzinger, E. and Smith, E. (2008). Information security management:An information security retrieval and awareness model for industry. *Computer & Security*, *27*, 224-231.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

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

Kuzu, A. (2008). *İnternet Kullanımı ve Aile Araştırması.* Ankara: T.C. Başbakanlık Aile ve Sosyal Araştırmalar Genel Müdürlüğü Yayınları.

KVKK. (2022). Kişisel Verilerin Korunması Kanunu. Erişim adresi: https://www.kvkk.gov.tr/

Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel psychology, 28*(4), 563-575.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671.

Lee, K., Caverlee, J. and Webb, S. (2010). *Uncovering social spammers: social honeypots+ machine learning.* In Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval (pp. 435-442).

Lee, L. (2002). Enhancing learners' communication skills through synchronous electronic interaction and task-based instruction. *Foreign Language Annals*, *35*(1), 16-24.

Lee, L. (2016). Autonomous learning through task-based instruction in fully online language courses. *Language Learning & Technology*, *20*(2), 81-97.

Leszczyna, R. (2018). A review of standards with cybersecurity requirements for smart grid. *Computers & security*, *77*, 262-276.

Li, Y., Zhang, N. and Siponen, M. (2019). Keeping secure to the end: a long-term perspective to understand employees' consequence-delayed information security violation. *Behaviour & Information Technology*, *38*(5), 435-453.

Long, M. (1985). A role for instruction in second language acquisition: Task-based language teaching. In K. Hylstenstam & M. Pienemann (eds.), *Modelling and Assessing Second Language Acquisition* (pp. 77-99).

Mahabi, V. (2010). *Information security awareness: System administrators and end-user perspectives at Florida State University*. Doctoral dissertation, The Florida State University, College of Communication and Information, Florida.

McAfee. (2019). Grand Theft Data. https://www.mcafee.com/enterprise/en-us/assets/infographics/infographic-data-exfiltration-2.pdf adresinden erişilmiştir.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151-156.

McCue, A. (2008). Beware the insider security threat, *CIO jury*.

McGartland, R. D., Berg-Weger, M., Tebb, S., Lee, E. S. and Rauch, S. (2003). "Objectifying content validity: Conducting a content validity study in social work research". *Social Work Research, 27*(2), 94-104.

McGriff, S. J. (2000). *Instructional System Design (ISD): Using the ADDIE Model,*

Mestçi, A. (2007), *"Türkiye'de İnternet Raporu 2007",* XII. Türkiye'de İnternet Konferansı, 8-10 Kasım 2007, Ankara, 175-183.

Metli, G. (2017). *Ortaokul Öğrencilerinin Siber Zorbalık, Siber Mağduriyet ve İnsani Değerleri Arasındaki İlişkinin İncelenmesi* (Kayıt No. 461389) [Yüksek Lisans Tezi, İstanbul Sabahattin Zaim Üniversitesi]. YÖK Tez Merkezi.

Mevzuat. (2022). Elektronik Haberleşme Kanunu. Erişim adresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5809&MevzuatTur=1&MevzuatTertip=5

Mochiko, T. (2016). *Cybercrime "will rise" with internet of things*. Business Live.

Muruganantham, G. (2015). Developing of e-content package by using ADDIE Model. *International Journal of Applied Research, 1*(3), 52-54.

Newcomb, L. H. and Treftz, M. K. (1987). Levels of cognition of students tests and assignments in the college of Agriculture at The Ohio State University. *Proceedings of the Central Region 41st Annual Research Conference in Agricultural Education*, Chicago, IL.

Nunan, D. (2004), *Task-based language teaching*, Cambridge Language Teaching Library.

Nunnally, J. C. (1978). *Psychometric testing.* New York: McGraw-Hill.

Nunnally, J. C. and Bernstein, I. (1994). *Psychometric theory.* New York: McGraw-Hill.

Ören, Z. (2021). *Türkçenin İkinci Dil Olarak Öğretiminde Bilgisayar Destekli Göreve Dayalı Yazma Öğretimi* (Kayıt No. 686443) [Doktora Tezi, Marmara Üniversitesi]. YÖK Tez Merkezi.

Özenç, K. (2007). *Bilgi ve iletişim teknolojilerinde kişisel ve kurumsal bilgi güvenliğinin sağlanması.* Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 13-14 Aralık 2007, Ankara.

Öztemiz, S. ve Yılmaz, B. (2013). Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği. *Bilgi Dünyası, 14*(1), 87-100.

Öztezcan, B. A. ve Çetinkaya, A. (2017). Bilgi güvenliği farkındalığı üzerine bir araştırma: Marmara Üniversitesi örneği. Ulusal Multidisipliner Hakemli. *Sosyal Bilimler ve Araştırmalar Dergisi*, *1*(1), 56-71.

Öztuna, D. ve Elhan, A.H. (2015). *Gruplar arası ve grup içi karşılaştırma yöntemleri.*

Pahnila, S., Siponen, M. and Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*.

Parlar, H. (2012). Bilgi toplumu, değişim ve yeni eğitim paradigması. *Yalova Sosyal Bilimler Dergisi*, *2*(4).

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, 165-176.

Pasquali, L. (2010). *Instrumentação psicológica: fundamentos e práticas*. PortoAlegre: Artmed

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., ve Calic, D. (2015). Factors that influence information security behavior: An Australian web-based study. *Human Aspects of Information Security, Privacy, and Trust*, 231-241.

Pools-m. (2013). Task Based Learning. Erişim Adresi: https://www.languages.dk/archive/pools-m/manuals/final/taskuk.pdf

Prabhu, N. S. (1987). *Second language pedagogy*. Oxford: Oxford University Press.

PricewaterhouseCoopers PwC (2016). *Turnaround and transformation in cybersecurity – Key findings from The Global State of Information Security Survey 2016*. https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf adresinden 20.01.2022 tarihinde erişildi.

Puhakainen, P. (2006). *A Design theory for information security awareness* (Kayıt No. 9514281144) [Doctoral Dissertation, Acta University of Oulu]. Jultika.

Qin, T. and Burgoon, J. K. (2007, May). An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In 2007 *IEEE Intelligence and Security Informatics* (pp. 152-159).

Rao, U. H and Nayak, U. (2014). *The InfoSec Handbook*. New York, Apress Media LLC.

Rasheed, M. I., Malik, M. J., Pitafi, A. H., Iqbal, J., Anser, M. K. and Abbas, M. (2020). Usage of social media, student engagement, and creativity: The role of knowledge sharing behavior and cyberbullying. *Computers & Education, 159*, 104002.

Rees, J., Bandyopadhyay, S. and Spafford, E. H. (2003). PFIRES: A policy framework for information security. *Communications of the ACM*, *46*(7), 101-106.

Reiser, R. A., and Dempsey, J. V. (2007). *Trends and issues in instructional design and technology* (4th ed.).Columbus, OH: Pearson

Rhee, H. S., Kim, C. and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & security*, *28*(8), 816-826.

Sarı, F. (2021). *Bilgi Güvenliğine Yönelik Çevrimiçi Eğitimin Ortaokul Öğrencilerinin Sanal Ortamlarda Bilgi Güvenliğine İlişkin Öğrenmelerine Etkisi* (Kayıt No. 705301) [Doktora Tezi, Hacettepe Üniversitesi]. YÖK Tez Merkezi.

Schermelleh-Engel, K. and Moosbrugger, H. (2003). Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research Online*, *8*(2),23-74.

Serter, B. (2021). *Ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeyinin belirlenmesi* (Kayıt No.679722) [Yüksek Lisans Tezi, Gazi Üniversitesi]. YÖK Tez Merkezi.

Sharma, S. and Aparicio, E. (2022). Organizational and Team Culture as Antecedents of Protection Motivation Among IT Employees. *Computers & Security*, *120*.

SimilarWeb. (2022). *Mobile app ranking.*

Sinha, A. K. Rai and B. Bhushan, "Information Security threats and attacks with conceivable counteraction", 2019 2nd International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), 2019.

Siponen, M. and Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502.

Siponen, M. T. (2001). Five Dimensions Of Information Security Awareness. *Computer and Society, 31*(2), 24-29.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S. and Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries. EU Kids Online.*

Solomon, A., Michaelshvili, M., Bitton, R., Shapira, B., Rokach, L., Puzis, R. and Shabtai, A. (2022). Contextual security awareness: A context-based approach for assessing the security awareness of users. *Knowledge-Based Systems*, *246*, 108709.

Spears, J. L. and Barki, H. (2010). User participation in information systems security risk management. *MIS quarterly*, 503-522.

Stahl, B. C., Doherty, N. F. and Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal*, *22*(1), 77-94.

Stanciu, V. and Tinca, A. (2016). Students' awareness on information security between own perception and reality–an empirical study. *Accounting and Management Information Systems*, *15*(1), 112-130.

Statista. (2022). *Statistics and market data on mobile internet & apps.*

Subramanya, S.R. and Lakshminarasimhan, N. (2001), "Computer Viruses", Potentials, *IEEE*, *20*(4), 16-19.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö. ve Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim*, *9*, 11-13.

Şahinaslan, E.,Kandemir, R. ve Şahinaslan, Ö.(2009). Bilgi Güvenliği Farkındalık Eğitim Örneği. *Akademik Bilişim Konferansı.* Şanlıurfa, 189-194.

Şendağ, S. ve Odabaşı. H. F. (2006). *İnternet ve Çocuk: Etik bunun neresinde*? 6. Uluslararası Eğitim Teknolojileri Konferansı Bildiri Kitapçığı (1508-1515). Gaziamağusa. KKTC, 19-21 Nisan.

Şimşek, Ö. F. (2007). *Yapısal eşitlik modellemesine giriş: Temel ilkeler ve LISREL uygulamaları.* Ankara: Ekinoks Yayınları

Tabachnick, B. G. and Fidell, L.v S. (2013). *Using multivariate statistics* (6. Ed.). Pearson, Boston

Tam, C., de Matos Conceição, C. and Oliveira, T. (2022). What influences employees to follow security policies?. *Safety science, 147,* 105595.

Tandoğan, M., Özer, B., Akkoyunlu, B., Kaya, Z., Odabaşı, F., Deryakulu, D. ve İmer, G. (1998). *Çağdaş eğitimde yeni teknolojiler*. Eskişehir: T.C.Anadolu Üniversitesi Açıköğretim Fakültesi Yayınları

Tavşancıl, E. (2005). *Tutumların ölçülmesi ve SPSS ile veri analizi.* Ankara: Nobel.

Tavşancıl. E. ve Aslan. E. A. (2001). *İçerik analizi ve Uygulama Örnekleri.* Ankara: Epsilon Yayınları.

Teker, E. (2019). *Öğretmenlerin ve Lise Öğrencilerinin Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi* (Kayıt No. 612885) [Yüksek Lisans Tezi, Ankara Üniversitesi]. YÖK Tez Merkezi.

Tekerek, M. (2008). Bilgi güvenliği yönetimi. *Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi, 11*(1), 132-137.

Tekerek, M. ve Tekerek, A. (2013). Öğrencilerin Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma. *Turkish Journal of Education*. *2*(3), 61-70.

Tezbaşaran, A. A., (2008). *Likert tipi ölçek geliştirme kılavuzu*. Ankara:TPD.

The One Brief. (2020). *The Key To A Holistic Cyber Security Program: The Human Element.* https://theonebrief.com/people-humans-cyber-greatest-risks/ adresinden erişilmiştir.

Theofanos, M., Choong, Y. Y. and Murphy, O. (2021). 'Passwords Keep Me Safe'–Understanding What Children Think about Passwords. *In 30th USENIX Security Symposium (USENIX Security 21)* (pp. 19-35).

Topa, I. and Karyda, M. (2019). From theory to practice: Guidelines for enhancing information security management. *Information and Computer Security, 27*(3), 326-342.

Torgerson, W. S. (1958). *Theory and methods of scaling.*

Türk Dil Kurumu. (2022). Türk Dil Kurumu Sözlükleri. Erişim adresi: https://www.sozluk.gov.tr/

Uslu, T. (2007). *İnternet güvenliği ve risk yönetimi*, Yayınlanmamış Yüksek Lisans Tezi. Kültür Üniversitesi FBE, İstanbul.

Van der Schyff, K. and Flowerday, S. (2021). Mediating effects of information security awareness. *Computers & Security*, *106*, 102313.

Veiga, A. D. (2008). *Cultivating and assessing information security culture* (Doctorate of Philosophy). University of Pretoria, Pretoria.

Veiga; A. D. and Eloff, J. H. P. (2010) "A Fremework and Assessment Instrument for Information Security Culture", *Computers & Security*, *29*, 198.

Veneziano L. and Hooper J. (1997). A method for quantifying content validity of health-related questionnaires. *American Journal of Health Behavior*, *21*(1), 67-70

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, *38*, 97-102.

Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri* (Kayıt No. 212815) [Yüksek Lisans Tezi, Gazi Üniversitesi]. YÖK Tez Merkezi.

Vural, Y. (2017). *ρ-kazanım: Mahremiyet korumalı fayda temelli veri yayınlama modeli* (Kayıt No. 478487) [Doktora Tezi, Hacettepe Üniversitesi]. YÖK Tez Merkezi.

Watkins, M. W. (2021). *A step-by-step guide to exploratory factor analysis with SPSS*. New York: Routledge.

Webster, F. (2014). *Theories of the information society*. Routledge.

Whitman, M. and Mattord, H. (2018*). Principles of Information Security. Boston*: Cengage Learning.

Wiley, A., McCormac, A. and Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101640.

Willis, D. and Willis, D. (2007). *Doing task-based teaching.* Oxford: OUP

Willis, J. (1996). A flexible framework for task-based learning. *Challenge and change in language teaching*, *52*, 62.

Wilson, F. R., Pan, W. and Schumsky, D. A. (2012). Recalculation of the critical values for Lawshe's content validity ratio. *Measurement and Evaluation in Counseling and Development*, *45*, 197–210.

Wu, T., Tien, K.-Y., Hsu, W.-C. and Wen, F.-H. (2021). Assessing the Effects of Gamification on Enhancing Information Security Awareness Knowledge. *Applied Sciences*, *11*(19), 9266.

Yenal, Ü. (2009). Bilgi Toplumunun Tarihçesi. *Tarih Okulu Dergisi*, 123-144.

Yeşilorman, M. ve Koç, F. (2016). Bilgi Toplumunun Teknolojik Temelleri Üzerine Eleştirel Bir Bakış. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, *24*(1), 117-133.

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

Yılmaz, H. (2015). *Örneklem büyüklüğünün saptanması ve istatistiksel testler.*

Yılmaz, K. ve Horzum, M. B. (2005). Küreselleşme, Bilgi Tekolojileri ve Üniversite. *İnönü Üniversitesi Eğitim Fakültesi Dergisi, 6*(10), 103-121.

Yılmaz, R., Karaoğlan Yılmaz F.G., Öztürk, H.T. ve Karademir T. (2017). Lise öğrencilerinin güvenli bilgisayar ve internet kullanım farkındalıklarının incelenmesi: Bartın ili örneği. *Pegem Eğitim ve Öğretim Dergisi*, *7*(1), 83-114.

Yılmaz, S. ve Salcan O., (2008). Siber Uzay'da Güvenlik ve Türkiye, 1. Basım, Milenyum Yayınları, İstanbul, 56-57.

Yoon, C., Hwang, J. W. and Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of information systems education*, *23*(4), 407-416.

Yurdagül, H. (2005). *Ölçek geliştirme çalışmalarında kapsam geçerliği için kapsam geçerlik indekslerinin kullanılması*. XVI. Ulusal Eğitim Bilimleri Kongresi içerisinde (1-6). Pamukkale Üniversitesi Eğitim Fakültesi. Denizli.

Zolotarev, V. V., Arkhipova, A. B., Kasimova, A. R., Maznina, Y. A. and Dyakonova, A. I. (2021). *Role and Task Based Model Adaptation for Security Awareness Game*. In 2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS) (pp. 773-777). IEEE.

Zwick, W. R. and Velicer, W. F. (1986). Comparison of five rules for determining the number of components toretain. *Psychological Bulletin, 99*(3), 432-442.

EKLER

(EK 1)

ORTAOKUL DÜZEYİ BİLGİ GÜVENLİĞİ FARKINDALIĞI ÖLÇEĞİ

Değerli Öğrenciler,

Bilgi güvenliği farkındalığının geliştirilmesinde görev temelli çevrimiçi öğrenme ortamının etkililiğini öğrenme amacıyla yapılan bu çalışmadan toplanacak bilgiler, bilimsel bir araştırma çerçevesinde kullanılacaktır. Bilgileriniz tamamen gizli tutulacak olup çalışmadaki ifadeleri tam ve içtenlikle doldurmanız araştırmanın sağlıklı ve güvenilir sonuçlara ulaşması açısından önem taşımaktadır.

Katkılarınız için şimdiden teşekkür ederim.

Lütfen soruları eksiksiz doldurunuz.

KİŞİSEL BİLGİLER

1. Cinsiyetiniz: (1) Kadın (2) Erkek

2. Yaşınız: (1) 10 (2) 11 (3) 12 (4) 13

3. Sınıfınız: (1) 5.sınıf (2) 6.sınıf (3) 7.sınıf (4) 8.sınıf

4. 2020-2021 karne not ortalamanız kaçtır?

(1) 45-55 (2) 55-70 (3) 70-85 (4) 85-100

5. Annenizin yaşı: **……** (1) *Bilmiyorum*

6. Babanızın yaşı: **……** (1) *Bilmiyorum*

7. Anne ve Babanızın eğitim durumu?

	İlkokul	**Ortaokul**	**Lise**	**Üniversite**	**Y.Lisans/ Doktora**
a. Annenizin	(1)	(2)	(3)	(4)	(5)
b. Babanızın	(1)	(2)	(3)	(4)	(5)

8. Ailenizin tahmini aylık geliri ne kadardır?

	0-2300	**2300-6000**	**6000-10000**	**10000 ve üzeri**	**Bilmiyorum**
a. Annenizin	(1)	(2)	(3)	(4)	(5)
b. Babanızın	(1)	(2)	(3)	(4)	(5)

9. Bilişim Teknolojilerine Yönelik Ders aldınız mı? (1) Evet (2) Hayır

9.1. Bir önceki soruya cevabınız evet ise bu eğitimi nereden aldınız?

(1) Okul (2) Kurs (3) Web Siteleri (4) Atölyeler(Kodlama, Deneyap)

9.2. Aldığınız bu eğitimi yeterli buluyor musunuz? (1) Evet (2) Hayır

10. Sosyal Medyayı hangi sıklıkla kullanırsınız?

(1) Hiçbir Zaman (2) Nadiren (3) Ara sıra (4) Çoğunlukla (5) Her zaman

11. Bilgisayarınızda virüs programı var mı?

12. Cevabınız evet ise lisanslı virüs programı mı kullanıyorsunuz? (1) Evet (2) Hayır

13. Aşağıdakilerin hangisine sahipsiniz ve hangi sıklıkla kullanmaktasınız?

	Sahibim		**Bu teknolojileri hangi sıklıkla kullanmaktasınız?**				
	Evet	**Hayır**	**Hiçbir zaman**	**Nadiren**	**Ara Sıra/Bazen**	**Çoğunlukla**	**Her Zaman**
a. Cep telefonu	(1)	(2)	(1)	(2)	(3)	(4)	(5)
b. Akıllı telefon	(1)	(2)	(1)	(2)	(3)	(4)	(5)
c. Akıllı saat	(1)	(2)	(1)	(2)	(3)	(4)	(5)
d. Tablet	(1)	(2)	(1)	(2)	(3)	(4)	(5)
e. Dizüstü bilgisayar	(1)	(2)	(1)	(2)	(3)	(4)	(5)
f. Masaüstü bilgisayar	(1)	(2)	(1)	(2)	(3)	(4)	(5)
g. Oyun konsolu (Playstation, Xbox vb.)	(1)	(2)	(1)	(2)	(3)	(4)	(5)
h. Hiçbiri	(1)	(2)	(1)	(2)	(3)	(4)	(5)
i. Diğer……	(1)	(2)	(1)	(2)	(3)	(4)	(5)

14. Aşağıdakilerin hangisine çevrenizdekilerle ortak sahipsiniz ve hangi sıklıkla kullanmaktasınız?

	Ortak Kullanıyorum		**Bu teknolojileri hangi sıklıkla kullanmaktasınız?**				
	Evet	**Hayır**	**Hiçbir zaman**	**Nadiren**	**Ara Sıra/Bazen**	**Çoğunlukla**	**Her Zaman**
a. Cep telefonu	(1)	(2)	(1)	(2)	(3)	(4)	(5)
b. Akıllı telefon	(1)	(2)	(1)	(2)	(3)	(4)	(5)
c. Akıllı saat	(1)	(2)	(1)	(2)	(3)	(4)	(5)
d. Tablet	(1)	(2)	(1)	(2)	(3)	(4)	(5)
e. Dizüstü bilgisayar	(1)	(2)	(1)	(2)	(3)	(4)	(5)
f. Masaüstü bilgisayar	(1)	(2)	(1)	(2)	(3)	(4)	(5)
g. Oyun konsolu (Playstation, Xbox vb.)	(1)	(2)	(1)	(2)	(3)	(4)	(5)
h. Hiçbiri	(1)	(2)	(1)	(2)	(3)	(4)	(5)
i. Diğer……	(1)	(2)	(1)	(2)	(3)	(4)	(5)

15. İnternete bağlanmak için kullandığınız cihazlar nelerdir ve ne sıklıkla bağlanırsınız?

	Ortak Kullanıyorum		Bu teknolojileri hangi sıklıkla kullanmaktasınız?				
	Evet	**Hayır**	**Hiçbir zaman**	**Nadiren**	**Ara Sıra/Bazen**	**Çoğunlukla**	**Her Zaman**
a. Cep telefonu	(1)	(2)	(1)	(2)	(3)	(4)	(5)
b. Akıllı telefon	(1)	(2)	(1)	(2)	(3)	(4)	(5)
c. Akıllı saat	(1)	(2)	(1)	(2)	(3)	(4)	(5)
d. Tablet	(1)	(2)	(1)	(2)	(3)	(4)	(5)
e. Dizüstü bilgisayar	(1)	(2)	(1)	(2)	(3)	(4)	(5)
f. Masaüstü bilgisayar	(1)	(2)	(1)	(2)	(3)	(4)	(5)
g. Oyun konsolu (Playstation, Xbox vb.)	(1)	(2)	(1)	(2)	(3)	(4)	(5)
h. Hiçbiri	(1)	(2)	(1)	(2)	(3)	(4)	(5)
i. Diğer……	(1)	(2)	(1)	(2)	(3)	(4)	(5)

16. İnterneti hangi amaçla ve ne sıklıkla kullanıyorsunuz?

	Hangi sıklıkla kullanmaktasınız?				
	Hiçbir zaman	**Nadiren**	**Ara Sıra/Bazen**	**Çoğunlukla**	**Her Zaman**
1. Arkadaşlarımla iletişim içinde olmak	(1)	(2)	(3)	(4)	(5)
2. Dersle ilgili konular hakkında yardım almak	(1)	(2)	(3)	(4)	(5)
3. Profesyonel ilişkiler kurmak	(1)	(2)	(3)	(4)	(5)
4. Yeni Arkadaşlar Edinmek	(1)	(2)	(3)	(4)	(5)
5. Oyun Oynamak	(1)	(2)	(3)	(4)	(5)
6. Güncel olayları takip etmek	(1)	(2)	(3)	(4)	(5)
7. Alışveriş Yapmak	(1)	(2)	(3)	(4)	(5)
8. Video İzlemek	(1)	(2)	(3)	(4)	(5)
9. Müzik dinlemek	(1)	(2)	(3)	(4)	(5)

ÖLÇEK MADDELERİ

Aşağıda bilgi güvenliği farkındalığına yönelik görüşlerinizi tanımlayan maddeler yer almaktadır. Aşağıdaki ifadelere ne derece katılıp-katılmadığınızı seçeneğin karşısındaki kutuya (X) işareti koyarak belirtiniz. Lütfen her soruyu dikkatli okuyunuz ve boş madde bırakmayınız.	Kesinlikle katılmıyorum	Katılmıyorum	Kısmen katılmıyorum	Katılıyorum	Kesinlikle katılıyorum
1. Üzerinde çalışma yapılan dosyaların birden fazla güvenli ortamda yedeklenmesi gerektiğini bilirim.	1)	2)	3)	4)	5)
2. Elektrik kesintisine karşı dizüstü bilgisayarları bataryası ile kullanmanın önemini bilirim.	1)	2)	3)	4)	5)
3. İnternet üzerinden gelen (e-posta, sosyal medya platformları) kimlik bilgilerini doğrulama mesajlarına (şifre, kredi kartı, kimlik bilgileri, vb.) itibar edilmemesi gerektiğini bilirim.	1)	2)	3)	4)	5)
4. Sahte içerikli posta (spam, önemsiz ve çöp) nedir bilirim?	1)	2)	3)	4)	5)
5. Sahte içerikli e-postaları engellemem gerektiğini bilirim.	1)	2)	3)	4)	5)
6. Tanımadığım kişilerden gelen e-postaları gereksiz e-posta (spam, önemsiz ve çöp) olarak işaretlemeye dikkat ederim.	1)	2)	3)	4)	5)
7. Şüpheli veya bilinmeyen kaynaklardan gelen e-postaları açmanın taşıdığı riski bilirim.	1)	2)	3)	4)	5)
8. Bilgisayarımın güvenliğini sağlayacak yazılımları bulma ve kullanma konusunda yeterli bilgiye sahibim.	1)	2)	3)	4)	5)
9. Şüpheli veya bilinmeyen kaynaklardan gelen e-postaları engellerim.	1)	2)	3)	4)	5)
10. İşletim sisteminin (Windows, Android, vb.) güncel olmasına dikkat ederim.	1)	2)	3)	4)	5)
11. İşletim sisteminin (Windows, Android, vb.) güvenlikle ilgili uyarılarını dikkate alırım.	1)	2)	3)	4)	5)
12. Güvenli olmadığını düşündüğüm e-postaları açmadan silmeye dikkat ederim.	1)	2)	3)	4)	5)
13. Sahte ya da yasal olmayan site adreslerini fark ederim.	1)	2)	3)	4)	5)
14. Yazılımları, üreticinin kendi sitesinden indirilmesinin önemini bilirim.	1)	2)	3)	4)	5)
15. Bilgisayarımda yasa dışı yolla edinilmiş (korsan) yazılımlar bulunmaması gerektiğini bilirim.	1)	2)	3)	4)	5)
16. Sosyal medya platformlarında kişisel bilgilerimi paylaşırım.	1)	2)	3)	4)	5)
17. Kişisel fotoğraf ve videolarımı herkesin erişebileceği ortamlarda paylaşırım.	1)	2)	3)	4)	5)
18. Göndereni tanımasam da tepkimi veya ilgimi çeken postaları yanıtlarım.	1)	2)	3)	4)	5)
19. İnternette ilgimi çeken reklamlara tıklarım.	1)	2)	3)	4)	5)
20. İnternette karşıma çıkan "tebrikler ödül kazandınız" vb. bildirimlere tıklarım.	1)	2)	3)	4)	5)
21. İnternette kaynağı belirsiz etkinliklere (anket, oyun, çekiliş, vb.) katılım sağlarım.	1)	2)	3)	4)	5)
22. Güvenli olmadığını düşündüğüm web sitelerine girdiğimde mikrofon, kamera ve konum bilgisi gibi erişim isteğine izin/onay veririm.	1)	2)	3)	4)	5)

23. Kişisel bilgilerimi (T.C. Kimlik numarası, ev veya iş adresi, vb.) internet ortamında talep edilen her yere veririm.	1)	2)	3)	4)	5)
24. İnternet ortamında para yardımı talep edenlere yardımda bulunurum.	1)	2)	3)	4)	5)
25. Yasaklı sitelere giriş yapmamam gerektiğini bilirim.	1)	2)	3)	4)	5)
26. Yasaklı sitelere giriş yapmamam gerektiğini bilirim.	1)	2)	3)	4)	5)
27. Çekiliş adı altında sunulan etkinliklere kişisel bilgilerimi vermemem gerektiğini bilirim.	1)	2)	3)	4)	5)
28. Paylaşım yaptığım gönderilere gelen uygunsuz veya şiddet içerikli yorumları silmem gerektiğini bilirim.	1)	2)	3)	4)	5)
29. Kullandığım bilişim teknolojilerinde (telefon, bilgisayar, tablet, vb) konum bilgilerini gerekmedikçe kapalı tutmam gerektiğini bilirim.	1)	2)	3)	4)	5)
30. Akıllı telefonuma şifre, parmak izi ya da yüz tanıma gibi güvenli bir yöntem ile giriş yaparım.	1)	2)	3)	4)	5)

EK 2

AÇIK UÇLU SORU FORMU

Soru 1. Geliştirilen Görev temelli çevrimiçi öğrenme ortamına yönelik görüşleriniz nelerdir? Açıklayınız.

……..……

……..……

……

Soru 2. Görev temelli çevrimiçi öğrenme ortamında eğitim aldığınız sürece yönelik görüşleriniz nelerdir? Açıklayınız.

……..……

……..……

……

Değerli katkılarınız için teşekkür ederiz.

EK-3 ÖLÇEK KULLANIM İZNİ

Bülent Öktelik 16:09 (5 dakika önce)

Merhaba hocam, İlköğretim Online, Lise öğrencileri için geliştirmiş olduğunuz ölçeği kullanmak için izin istiyorum. Selamınızı iletiyorum, umarım sizinle tanışm

Can GÜLDÜREN 16:13 (0 dakika önce)

Alıcı: ben

Bülent merhaba,

İstemiş olduğun ölçek detaylarına ekli dosyadan ulaşabilirsin. Çalışma sonuçlarını paylaşırsan sevinirim.

Ben de sizinle tanışmak isterim.

Ölçek Açıklamaları:
Ölçek 14-18 yaş arası Lise (K12) öğrencileri üzerinde geliştirilmiştir. Ölçekte ters kodlanmış madde yoktur. Ölçek toplam puanı ve alt faktörlere ilişkin puanlar attıkça, katılımcıların Bilgi Güvenliği Farkındalığı artmaktadır.

Bilgi Güvenliği Ölçek Faktör Yapısı: Kişisel Verilerin Korunması: 1-6, Saldırı ve Tehditler: 7- 25, Mahremiyet: 26-36

Kolay gelsin.
İyi çalışmalar

EK – 4 ÖLÇEK KULLANIM İZNİ

ÖZCAN ERKAN AKGÜN 12 Ara 2020 Cmt 13:06

Alıcı: ben

Merhaba Bülent Bey,
Bilimsel çalışmalarınızda, etik ve raporlama kurallarına uygun şekilde çalışmamızdan yararlanmanızdan mutluluk duyarız.
İyi çalışmalar ve başarılar dilerim. Levent Hoca'ya selamlar
Özcan Erkan Akgün

From: Bülent Öktelik
Sent: Friday, December 11, 2020 22:49
To: ÖZCAN ERKAN AKGÜN
Subject: Re: Bilişim Güvenliği Anketi Kullanım İzni

Sayın Doç. Dr. Özcan Erkan Akgün Hocam merhaba,

Çanakkale Onsekiz Mart Üniversitesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümünde Yüksek Lisans Öğrencisiyim ve Doç. Dr. Levent Çetinkaya'nın danışmanlığında tez çalışmamı yürütmekteyim. Tez çalışmamızda kullanmak üzere geliştirmiş olduğunu "Bilişim Güvenliği Anketi" ve anket yer alan maddelerden yararlanmak için izninizi istiyorum. Şimdiden katkı ve destekleriniz için çok teşekkür ederim.

Saygılarımla. İyi günler dilerim.

EK-5 ETİK KURUL ONAYI

T.C.
ÇANAKKALE ONSEKİZ MART ÜNİVERSİTESİ REKTÖRLÜĞÜ
Lisansüstü Eğitim Enstitüsü
Lisansüstü Eğitim Enstitüsü Etik Kurulu

Sayı : E-84026528-050.01.04-2100058562 15.04.2021
Konu : Başvuru İncelenmesi

Sayın Bülent ÖKTELİK

Yürütücülüğünüzü yapmış olduğunuz 2021- YÖNP-0233 nolu Projeniz ile ilgili Bilimsel Araştırmalar Etik Kurulu'nun almış olduğu 08.04.2021 tarih ve 07/10 sayılı kararı aşağıdadır.
Bilgilerinize rica ederim.

KARAR:10- Bülent ÖKTELİK'in sorumlu yürütücülüğünü yaptığı "Bilgi güvenliği farkındalığının geliştirilmesinde görev temelli çevrimiçi öğrenme ortamının etkililiği" başlıklı araştırmasının Bilimsel Araştırma Etik Kurul ilkelerine **uygun olduğuna** oy birliği ile karar verilmiştir.

Prof. Dr. Salih Zeki GENÇ
Kurul Başkanı

Bu belge, güvenli elektronik imza ile imzalanmıştır.
Belge Doğrulama Kodu: DF4PEF4 Belge Takip Adresi: dogrulama.comu.edu.tr

Adres: Onsekiz Mart Üniversitesi Terzioğlu Yerleşkesi Çanakkale
Telefon No io:
e-Posta:
Kep Adresi:

Bilgi için : Halime Karadağ
Fen Bilimleri Enstitüsü Etik Kurulu Memur
Telefon No:

1/1

EK 6- ANKET OLURU

T.C.
ÇANAKKALE VALİLİĞİ
İl Millî Eğitim Müdürlüğü

Sayı : E-60305806-44-33806184 05.10.2021
Konu : Anket Çalışması (Bülent ÖKTELİK)

MİLLÎ EĞİTİM MÜDÜRLÜĞÜNE
ÇANAKKALE

İlgi :Çanakkale Onsekiz Mart Üniversitesi Öğrenci İşleri Daire Başkanlığının 16/09/2021 tarihli ve 2100166943 sayılı yazısı.

Çanakkale Onsekiz Mart Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Yüksek Lisans Programı öğrencisi Bülent ÖKTELİK'in, "Bilgi Güvenliği Farkındalığının Geliştirilmesinde Görev Temelli Çevrimiçi Öğrenme Ortamının Etkililiği" konulu tez çalışması kapsamında anket/ölçek çalışmasının, 2021-2022 Eğitim Öğretim yılında, Çanakkale merkez ilçedeki ekli listede belirtilen resmi/özel ortaokullarda öğrenim gören öğrencilere denetimi ilgili okul/kurum müdürlüğünde olmak üzere, kurum faaliyetlerini aksatmadan, gönüllülük esasına göre yüz yüze eğitimin devam etmesi halinde yüz yüze, uzaktan eğitimin devam etmesi durumunda çevrimiçi (online) yapılma isteği, Müdürlüğümüz Anket-Araştırma İnceleme Komisyonunca incelenerek uygun görülmüştür.

Makamlarınızca da uygun görüldüğü takdirde, Olurlarınıza arz ederim.

Hasan ERGÜVEN
Şube Müdürü

OLUR
Ferhat YILMAZ
Millî Eğitim Müdürü

Güvenli Elektronik İmzalı
Aslı ile aynıdır

Ek :
1-Komisyon Raporu (01 Sayfa)
2-Onaylı Veri Toplama Araçları (17 Sayfa)

EK 7- ZORLUK DÜZEYİNE GÖRE GÖREVLER VE HAFTALIK GÖRÜNÜMÜ

GÖREV NO	GÖREV	ZORLUK SEVİYESİ
1.	Arkadaşınız sizden bir fotoğrafa bakmak için sosyal medya hesabınıza girmek istemektedir. Bunun için sizden kullanıcı adı ve şifrenizi istemesi durumunda arkadaşınıza cevabınız ne olur?	Çok Kolay
2.	Bir öğretmeninize bilgi güvenliği kavramını sorunuz ve verdiği cevabı sisteme giriniz.	Çok Kolay
3.	Bülent ödevini yapmak için internet kafeye gitmiştir, İnternette kafede hazırladığı ödevi öğretmenine e-posta ile göndermek istemektedir. Bu aşamada dikkat etmesi gerekenler nelerdir? En az 3 tane yazınız.	Çok Kolay
4.	Siber zorbalık ile ilgili 3 video bulunuz ve video bağlantılarını sisteme yükleyiniz.	Çok Kolay
5.	Ailenize sosyal medya hesaplarının çalınması durumunda neler yapması gerektiğini sorunuz ve ailenizden gelen cevapları sisteme giriniz.	Kolay
6.	Aşağıda bulunan fotoğrafa iyi bir dijital yurttaşın özelliklerini aileniz ile doldurup sisteme yükleyiniz. (EK-2)	Kolay
7.	Aşağıda bulunan hikâyeyi ailenize okuyunuz. Daha sonra aileniz ile hikâyede bulunan bilgi güvenliği ihlallerini tespit edip sisteme giriniz. (EK-1)	Kolay
8.	Okulunuza yeni gelen bir arkadaşınız, sınıf arkadaşlarınız tarafından sosyal medya üzerinden kırıcı ve aşağılayıcı bir mesaja maruz kalırsa tepkiniz ne olur? Lütfen cevabınızı sisteme giriniz.	Kolay
9.	EK-3' te bulunan Sezar Şifresi fotoğrafına bakarak aşağıdaki 3 şifreyi çözünüz. (EK-3) 1. Bilim (……) 2. Etik (……) 3. Bilgisayar (……)	Zor
10.	Aşağıda bulunan e-posta örneklerini ailenize gösteriniz ve bu e-postalardaki tuzakları tespit ederek yapılması gerekenleri sisteme giriniz. (EK-5)	Zor
11.	Aşağıdaki verilen kriterler doğrultusunda en güçlü şifreyi oluşturduktan sonra sisteme giriniz. • Oluşturacağınız şifre Minimum 8, Maksimum 20 karakter olmalı, • Oluşturacağınız şifrede bir özel karakter, en az 2 sayı olmalı • Oluşturacağınız şifrede A, E ve S harfleri olmak zorundadır.	Zor
12.	Okulunuzda veya mahallenizde bir arkadaşınıza "Tebrikler Ödül Kazandınız, lütfen bu bağlantıya tıklayın!" mesajı ile karşılaşmaları durumunda ne yapacaklarını sorun ve cevapları sisteme giriniz.	Zor
13.	Aşağıda bulunan web sitelerden 2 tanesini seçip EK- 7 de bulunan formu doldurunuz. Doldurduğunuz görseli sisteme yükleyiniz. 1. https://www.meb.gov.tr/ 2. https://kesfetprojesi.org/ 3. https://bilgeis.net/#/ 4. https://3dedi.com/	Çok Zor
14.	Bir arkadaşınız, anlık mesajlaşma uygulaması (whatsapp, telegram vb.) üzerinden size "Hemen üye ol, büyük ödülü sen kazan!" şeklinde bir mesaj gönderip üye olmanızı istedi. Bu mesaja tepkiniz ne olur? Lütfen cevabı sisteme giriniz.	Çok Zor
15.	Bilgi Güvenliği kavramı ile ilgili bilgilendirici bir broşür veya afiş hazırlayıp sisteme yükleyiniz.	Çok Zor
16.	Şifresiz (herkese açık) bir kablosuz ağa bağlanma konusunda herhangi bir sıkıntı olmadığını düşünen 3 arkadaşınızı tespit ediniz. Bu arkadaşlarınıza bu ağların risklerine yönelik bilgilendirme yapınız. Konu hakkında EK 4'te detaylı bilgiye ulaşabilirsiniz.	Çok Zor

1. HAFTA GÖREVLERİ

Siber zorbalık ile ilgili 3 video bulunuz ve video bağlantılarını sisteme yükleyiniz.	**Çok Kolay**
Aşağıda bulunan fotoğrafa iyi bir dijital yurttaşın özelliklerini aileniz ile doldurup sisteme yükleyiniz. (EK-2)	**Kolay**
Aşağıdaki verilen kriterler doğrultusunda en güçlü şifreyi oluşturduktan sonra sisteme giriniz. • Oluşturacağınız şifre Minimum 8, Maksimum 20 karakter olmalı, • Oluşturacağınız şifrede bir özel karakter, en az 2 sayı olmalı • Oluşturacağınız şifrede A, E ve S harfleri olmak zorundadır.	**Zor**
Bir arkadaşınız, anlık mesajlaşma uygulaması (whatsapp, telegram vb.) üzerinden size "Hemen üye ol, büyük ödülü sen kazan!" şeklinde bir mesaj gönderip üye olmanızı istedi. Bu mesaja tepkiniz ne olur? Lütfen cevabı sisteme giriniz.	**Çok Zor**

2. HAFTA GÖREVLERİ

Arkadaşınız sizden bir fotoğrafa bakmak için sosyal medya hesabınıza girmek istemektedir. Bunun için sizden kullanıcı adı ve şifrenizi istemesi durumunda arkadaşınıza cevabınız ne olur?	**Çok Kolay**
Aşağıda bulunan hikâyeyi ailenize okuyunuz. Daha sonra aileniz ile hikâyede bulunan bilgi güvenliği ihlallerini tespit edip sisteme giriniz. (EK-1)	**Kolay**
EK-3' te bulunan Sezar Şifresi fotoğrafına bakarak aşağıdaki 3 şifreyi çözünüz. (EK-3) Bilim (……) Etik (……) Bilgisayar (……)	**Zor**
Bilgi Güvenliği kavramı ile ilgili bilgilendirici bir broşür veya afiş hazırlayıp sisteme yükleyiniz.	**Çok Zor**

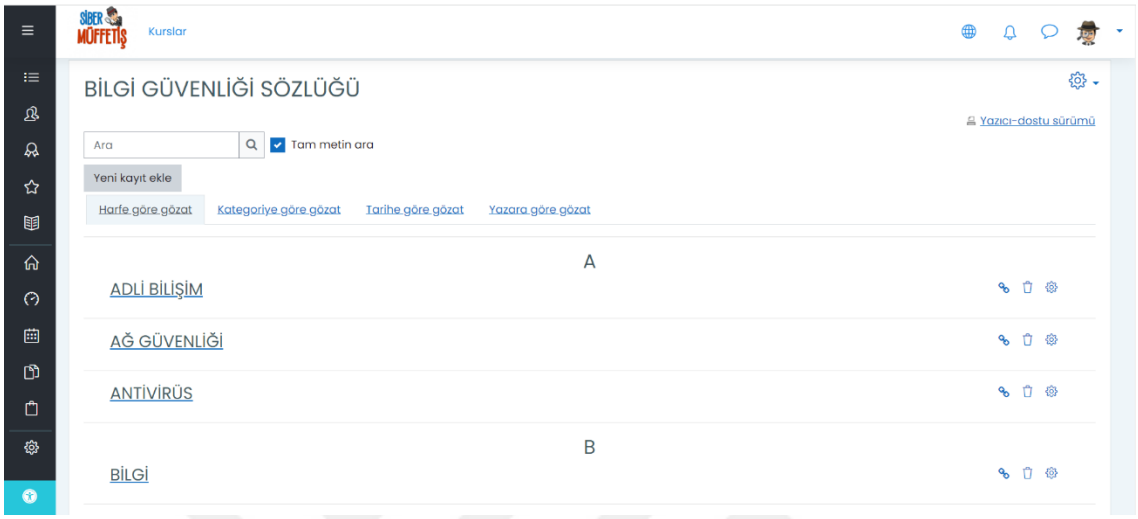
3. HAFTA GÖREVLERİ

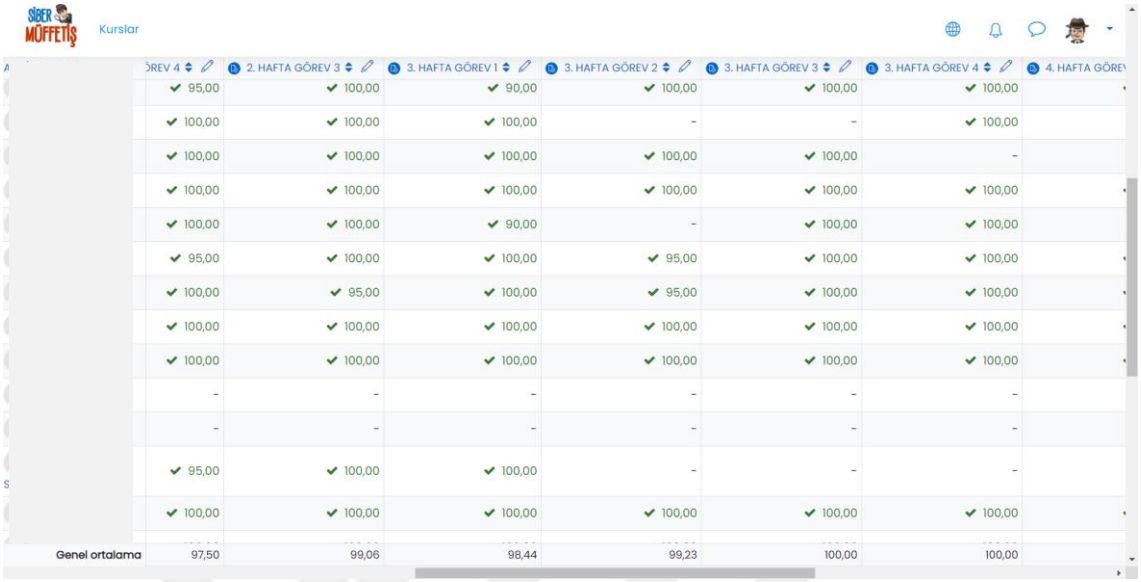
Bülent ödevini yapmak için internet kafeye gitmiştir, İnternette kafede hazırladığı ödevi öğretmenine e-posta ile göndermek istemektedir. Bu aşamada dikkat etmesi gerekenler nelerdir? En az 3 tane yazınız.	**Çok Kolay**
Ailenize sosyal medya hesaplarının çalınması durumunda neler yapması gerektiğini sorunuz ve ailenizden gelen cevapları sisteme giriniz.	**Kolay**
Aşağıda bulunan e-posta örneklerini ailenize gösteriniz ve bu e-postalardaki tuzakları tespit ederek yapılması gerekenleri sisteme giriniz. (EK-5)	**Zor**
Aşağıda bulunan web sitelerden 2 tanesini seçip EK- 7 de bulunan formu doldurunuz. Doldurduğunuz görseli sisteme yükleyiniz. 1. https://www.meb.gov.tr/ 2. https://kesfetprojesi.org/ 3. https://bilgeis.net/#/ 4. https://3dedi.com/	**Çok Zor**

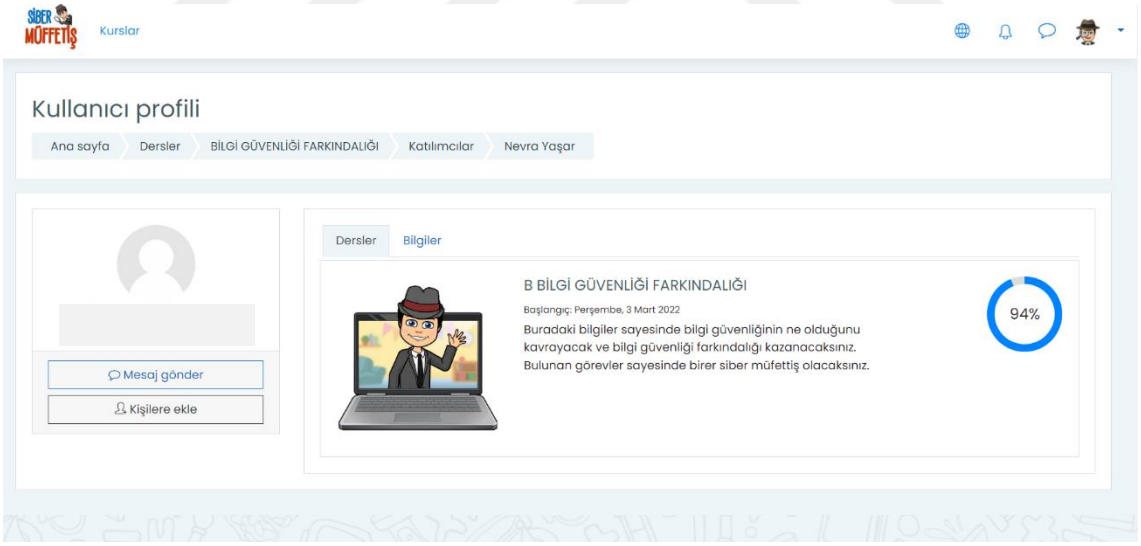
4. HAFTA GÖREVLERİ

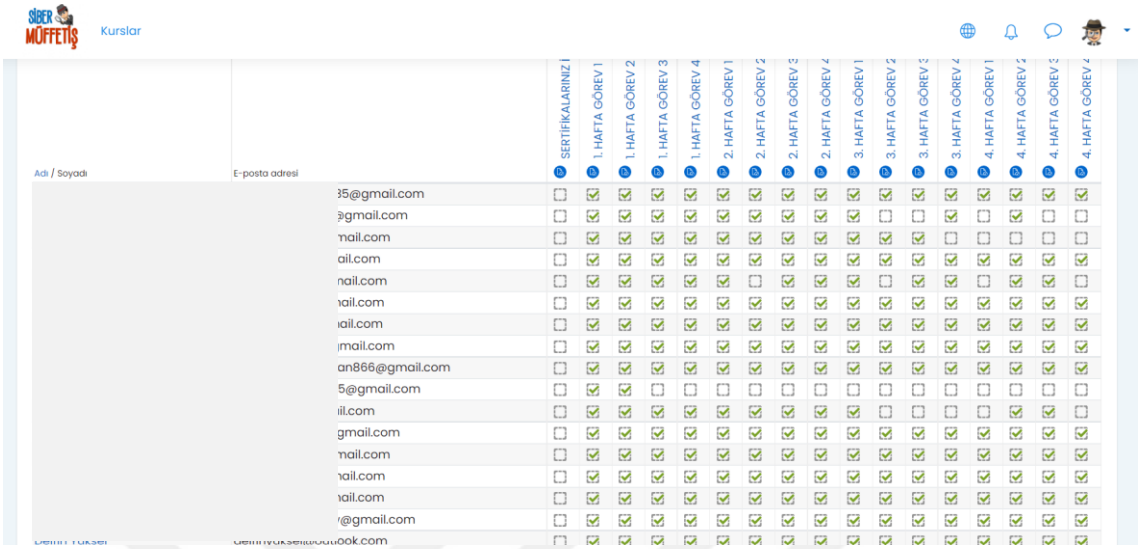
Bir öğretmeninize bilgi güvenliği kavramını sorunuz ve verdiği cevabı sisteme giriniz.	**Çok Kolay**
Okulunuza yeni gelen bir arkadaşınız, sınıf arkadaşlarınız tarafından sosyal medya üzerinden kırıcı ve aşağılayıcı bir mesaja maruz kalırsa tepkiniz ne olur? Lütfen cevabınızı sisteme giriniz.	**Kolay**
Okulunuzda veya mahallenizde bir arkadaşınıza "Tebrikler Ödül Kazandınız, lütfen bu bağlantıya tıklayın!" mesajı ile karşılaşmaları durumunda ne yapacaklarını sorun ve cevapları sisteme giriniz.	**Zor**
Şifresiz (herkese açık) bir kablosuz ağa bağlanma konusunda herhangi bir sıkıntı olmadığını düşünen 3 arkadaşınızı tespit ediniz. Bu arkadaşlarınıza bu ağların risklerine yönelik bilgilendirme yapınız. Bilgilendirme yaptığınıza dair EK-6'daki formu bilgilendirdiğiniz arkadaşlarınıza doldurup sisteme yükleyiniz. Konu hakkında EK 4'te detaylı bilgiye ulaşabilirsiniz.	**Çok Zor**

EK 8 – ÖĞRENME ORTAMI EKRAN GÖRÜNTÜLERİ

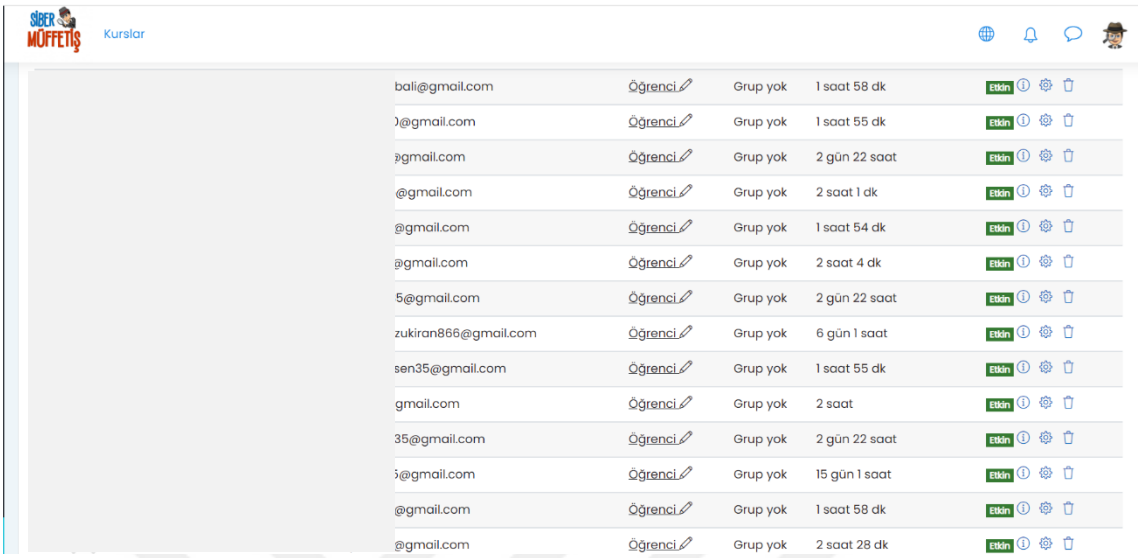


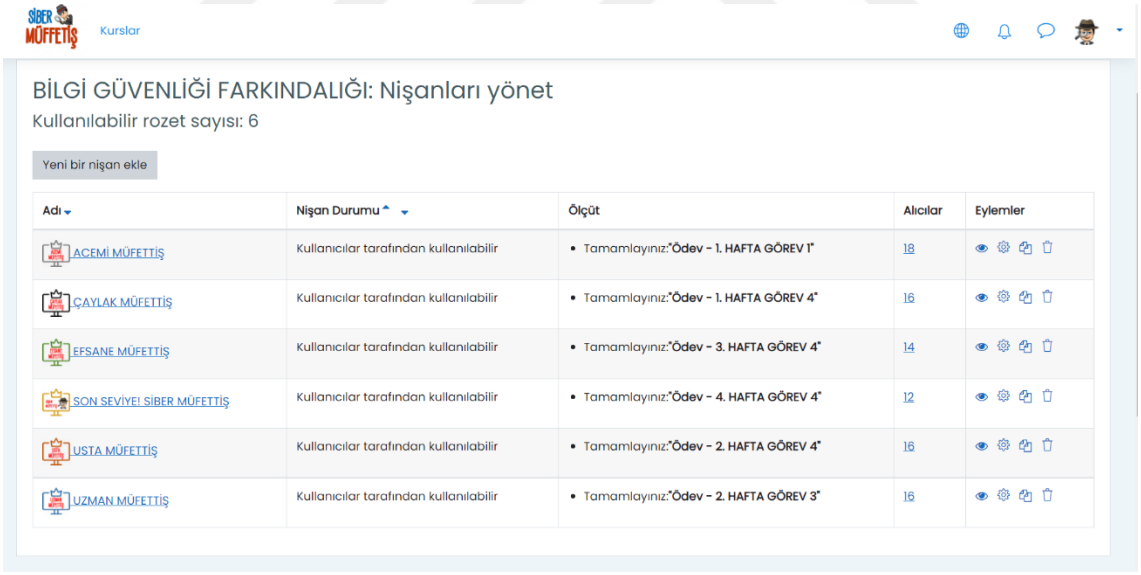

SİBER MÜFETTİŞ
Kurslar
2. HAFTA GÖREV 3
3. HAFTA GÖREV 1
3. HAFTA GÖREV 2
3. HAFTA GÖREV 3
3. HAFTA GÖREV 4
4. HAFTA GÖRE
Genel ortalama
97,50
99,06
98,44
99,23
100,00
100,00

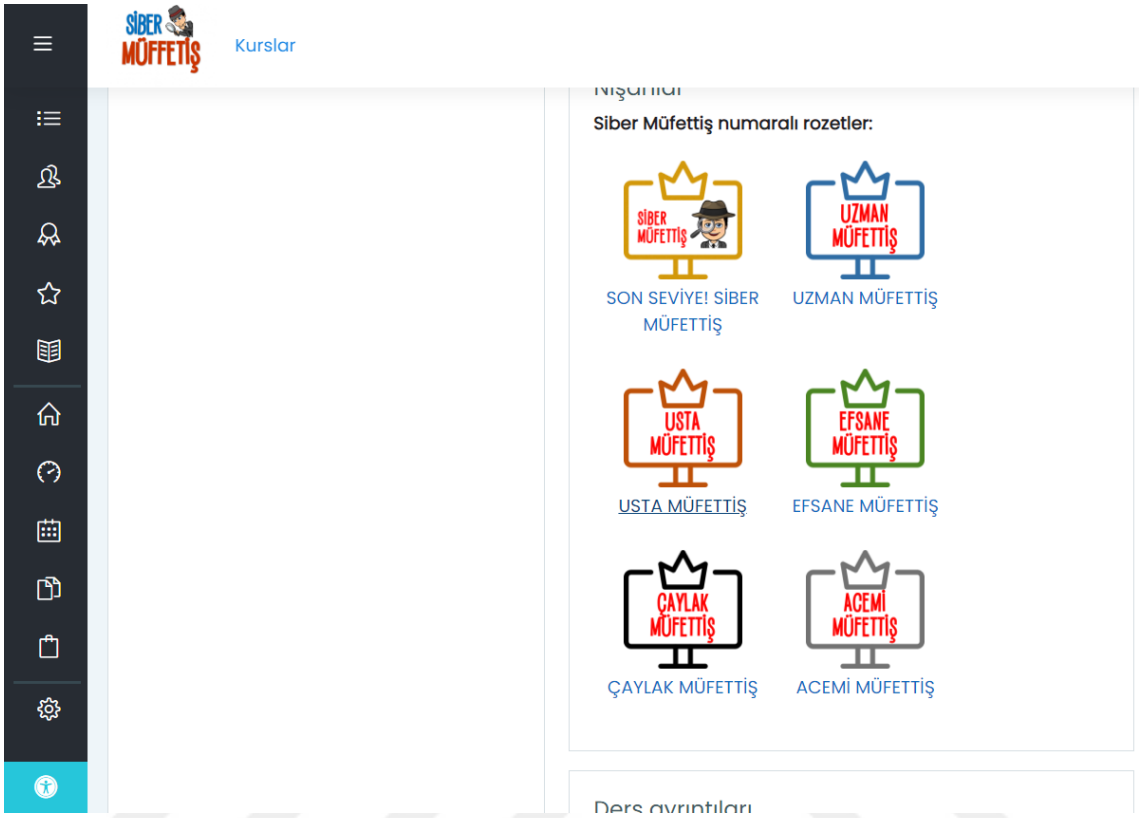

SİBER MÜFETTİŞ
Kurslar
Kullanıcı profili
Ana sayfa
Dersler
BİLGİ GÜVENLİĞİ FARKINDALIĞI
Katılımcılar
Nevra Yaşar
Mesaj gönder
Kişilere ekle
Dersler
Bilgiler
B BİLGİ GÜVENLİĞİ FARKINDALIĞI
Başlangıç: Perşembe, 3 Mart 2022
Buradaki bilgiler sayesinde bilgi güvenliğinin ne olduğunu kavrayacak ve bilgi güvenliği farkındalığı kazanacaksınız. Bulunan görevler sayesinde birer siber müfettiş olacaksınız.
94%


Kurslar
Adı / Soyadı
E-posta adresi
SERTİFİKALARINIZ
1. HAFTA GÖREV 1
1. HAFTA GÖREV 2
1. HAFTA GÖREV 3
1. HAFTA GÖREV 4
2. HAFTA GÖREV 1
2. HAFTA GÖREV 2
2. HAFTA GÖREV 3
2. HAFTA GÖREV 4
3. HAFTA GÖREV 1
3. HAFTA GÖREV 2
3. HAFTA GÖREV 3
3. HAFTA GÖREV 4
4. HAFTA GÖREV 1
4. HAFTA GÖREV 2
4. HAFTA GÖREV 3
4. HAFTA GÖREV 4


Güvenli değil | sibermufettis.com/moodle/mod/assign/view.php?id=11&forceview=1
Kurslar
BİLGİ GÜVENLİĞİ FARKINDALIĞI
Ana sayfa
Dersler
BİLGİ GÜVENLİĞİ FARKINDALIĞI
3.HAFTA GÖREVLERİ
3. HAFTA GÖREV 1
3. HAFTA GÖREV 1
Açıldı: Çarşamba, 2 Mart 2022, 12:00 ÖÖ
Gönderim yap
Receive a grade
Bülent ödevini yapmak için internet kafeye gitmiştir, İnternette kafede hazırladığı ödevi öğretmenine e-posta ile göndermek istemektedir. Bu aşamada dikkat etmesi gerekenler nelerdir? En az 3 tane yazınız.
Notlandırma özeti
Öğrencilerden gizli
Hayır
Katılımcılar
18
Gönderilen
16


SİBER MÜFETTİŞ
Kurslar
bali@gmail.com Öğrenci Grup yok 1 saat 58 dk Etkin
)@gmail.com Öğrenci Grup yok 1 saat 55 dk Etkin
gmail.com Öğrenci Grup yok 2 gün 22 saat Etkin
@gmail.com Öğrenci Grup yok 2 saat 1 dk Etkin
@gmail.com Öğrenci Grup yok 1 saat 54 dk Etkin
@gmail.com Öğrenci Grup yok 2 saat 4 dk Etkin
5@gmail.com Öğrenci Grup yok 2 gün 22 saat Etkin
zukiran866@gmail.com Öğrenci Grup yok 6 gün 1 saat Etkin
sen35@gmail.com Öğrenci Grup yok 1 saat 55 dk Etkin
gmail.com Öğrenci Grup yok 2 saat Etkin
35@gmail.com Öğrenci Grup yok 2 gün 22 saat Etkin
@gmail.com Öğrenci Grup yok 15 gün 1 saat Etkin
@gmail.com Öğrenci Grup yok 1 saat 58 dk Etkin
@gmail.com Öğrenci Grup yok 2 saat 28 dk Etkin


SİBER MÜFETTİŞ
Kurslar
BİLGİ GÜVENLİĞİ FARKINDALIĞI: Nişanları yönet
Kullanılabilir rozet sayısı: 6
Yeni bir nişan ekle
Adı
Nişan Durumu
Ölçüt
Alıcılar
Eylemler
ACEMİ MÜFETTİŞ Kullanıcılar tarafından kullanılabilir • Tamamlayınız:"Ödev - 1. HAFTA GÖREV 1" 18
ÇAYLAK MÜFETTİŞ Kullanıcılar tarafından kullanılabilir • Tamamlayınız:"Ödev - 1. HAFTA GÖREV 4" 16
EFSANE MÜFETTİŞ Kullanıcılar tarafından kullanılabilir • Tamamlayınız:"Ödev - 3. HAFTA GÖREV 4" 14
SON SEVİYE! SİBER MÜFETTİŞ Kullanıcılar tarafından kullanılabilir • Tamamlayınız:"Ödev - 4. HAFTA GÖREV 4" 12
USTA MÜFETTİŞ Kullanıcılar tarafından kullanılabilir • Tamamlayınız:"Ödev - 2. HAFTA GÖREV 4" 16
UZMAN MÜFETTİŞ Kullanıcılar tarafından kullanılabilir • Tamamlayınız:"Ödev - 2. HAFTA GÖREV 3" 16


SİBER MÜFFETİŞ
Kurslar
Siber Müfettiş numaralı rozetler:
SİBER MÜFETTİŞ
SON SEVİYE! SİBER MÜFETTİŞ
UZMAN MÜFETTİŞ
UZMAN MÜFETTİŞ
USTA MÜFETTİŞ
USTA MÜFETTİŞ
EFSANE MÜFETTİŞ
EFSANE MÜFETTİŞ
ÇAYLAK MÜFETTİŞ
ÇAYLAK MÜFETTİŞ
ACEMİ MÜFETTİŞ
ACEMİ MÜFETTİŞ