ÜNİVERSİTE ÖĞRENCİLERİNİN DİJİTAL GÜVENLİK ÖZ YETERLİKLERİ VE ÇEVRİMİÇİ RİSK ALMA EĞİLİMLERİNİN İNCELENMESİ

Doktora Tezi

Canan ÇOLAK

Eskişehir 2019

ÜNİVERSİTE ÖĞRENCİLERİNİN DİJİTAL GÜVENLİK ÖZ YETERLİKLERİ VE ÇEVRİMİÇİ RİSK ALMA EĞİLİMLERİNİN İNCELENMESİ

Canan ÇOLAK

DOKTORA TEZİ

Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı

Danışman: Doç. Dr. Işıl KABAKÇI YURDAKUL

İkinci Danışman: Dr. Öğr. Üyesi Onur DÖNMEZ

Eskişehir

Anadolu Üniversitesi

Eğitim Bilimleri Enstitüsü

Mayıs 2019

Bu tez çalışması TÜBİTAK BİDEB 2211 Yurtiçi Lisansüstü Eğitimi Destekleme Bursları tarafından desteklenmiştir. Ayrıca BAP komisyonu tarafından kabul edilen 1709E491 no.lu genel amaçlı proje kapsamında desteklenmiştir.

JÜRİ VE ENSTİTÜ ONAYI

Canan ÇOLAK'ın "Üniversite Öğrencilerinin Dijital Güvenlik Öz Yeterlikleri ve Çevrimiçi Risk Alma Eğilimlerinin İncelenmesi" başlıklı tezi 27.05.2019 tarihinde aşağıdaki jüri tarafından değerlendirilerek "Anadolu Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği"nin ilgili maddeleri uyarınca Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı Bilgisayar ve Öğretim Teknolojileri Öğretmenliği Programında, Doktora tezi olarak kabul edilmiştir.

	Unvanı-Adı Soyadı	İmza
Üye (Tez Danışmanı)	: Doç.Dr. Işıl KABAKÇI YURDAKUL	.....
Üye	: Prof.Dr. Ümit GİRGİN	.....
Üye	: Doç.Dr. Yusuf Levent ŞAHİN	.....
Üye	: Doç.Dr. Bahar BARAN	.....
Üye	: Doç.Dr. Ahmet Naci ÇOKLAR	.....

Doç.Dr. Yasemin ERGENEKON
Anadolu Üniversitesi
Eğitim Bilimleri Enstitüsü
Müdür Vekili

ÖZET

ÜNİVERSİTE ÖĞRENCİLERİNİN DİJİTAL GÜVENLİK ÖZ YETERLİKLERİ VE ÇEVRİMİÇİ RİSK ALMA EĞİLİMLERİNİN İNCELENMESİ

Canan ÇOLAK
Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı
Anadolu Üniversitesi, Eğitim Bilimleri Enstitüsü, Mayıs 2019
Danışman: Doç. Dr. Işıl KABAKÇI YURDAKUL
İkinci Danışman: Dr. Öğr. Üyesi Onur DÖNMEZ

Hayatın her alanında vazgeçilmez kolaylıklar sunan internet teknolojileri, bireylerin iyi oluşlarını etkileyen çeşitli riskleri de beraberinde getirmektedir. Söz konusu teknolojilerin kullanım süreleri ve kullanıcı sayıları arttıkça, dijital güvenliğin nasıl sağlanması gerektiği ve bu konuda hangi değişkenlerin incelenmesi gerektiği bilimsel araştırmalara konu olmuştur. Bu çalışmada üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin geçmişteki çevrimiçi risk alma eğilimleri ve dijital güvenlik öz yeterlikleri tarafından yordanma durumu ile şimdiki çevrimiçi risk alma eğilimleri ve dijital güvenlik öz yeterliklerinin farklı demografik özellikleri açısından incelenmesi amaçlanmıştır. Araştırma tekil ve ilişkisel tarama ile desenlenmiştir. Araştırmanın katılımcılarını 2017-2019 öğretim yılları süresince Eskişehir ili devlet üniversitelerinde öğrenim gören 1601 üniversite öğrencisi oluşturmuştur. Araştırma sürecinde Dijital Güvenlik Öz Yeterlik ve Çevrimiçi Risk Alma Eğilimi ölçekleri geliştirilmiş, bu ölçeklerin geçerlik ve güvenirlik çalışmaları yapılmıştır. Geliştirilen bu ölçekler aynı zamanda demografik bilgi formuyla birlikte araştırmanın veri toplama araçlarını oluşturmuştur. Veriler betimsel ve ilişkisel veri analizi teknikleriyle çözümlenmiştir. Üniversite öğrencilerinin dijital güvenlik öz yeterliklerinin yüksek düzeyde, çevrimiçi risk alma eğilimlerinin ise düşük sıklıkta olduğu belirlenmiştir. Cinsiyet, internet kullanım sıklığı ve yaş gruplarına göre dijital uygulamalarda güvenlik düzeyleri ve ticari riskler eğilimlerinde farklılıklar elde edilmiştir. Geçmişteki çevrimiçi risk eğilimleri boyutlarının ise şimdiki çevrimiçi risk alma eğilimlerini yordadığı sonucuna ulaşılmıştır.

Anahtar Sözcükler: Dijital Güvenlik, Çevrimiçi Riskler, Çevrimiçi Risk Alma Eğilimi, Üniversite Öğrencileri

ABSTRACT

INVESTIGATION OF DIGITAL SAFETY COMPETENCIES AND ONLINE RISK TAKING PROPENSITY OF UNIVERSITY STUDENTS

Canan ÇOLAK

Computer Education & Instructional Technology Department

Anadolu University, Graduate School of Educational Sciences, May 2019

Supervisor: Assoc. Prof. Dr. Işıl KABAKÇI YURDAKUL

Co-Supervisor: Assist. Prof. Dr. Onur DÖNMEZ

Internet technologies, which provide indispensable facilities in every aspect of life, bring with them various risks affecting the well-being of individuals. As the duration of usage of these technologies and number of users increased, how digital security should be ensured and what variables should be examined in this subject has been the subject of scientific research. This study aims to examine the extent to which current online risk-taking propensity of university students predicts their prior online risk-taking propensities and digital safety self-efficacy levels. Additionally, this study investigates the relations between current online risk-taking propensity and digital safety self-efficacy levels of university students in terms of various demographics. The study was designed with cross sectional survey designs. The required data were collected from 1601 university students studying at different state universities in Eskişehir, Turkey during 2017-2019 academic years. Within the scope of the study, valid and reliable Digital Safety Self-Efficacy and Online Risk-Taking Propensity scales were developed. These scales were also used as the data collection tools with demographic data form. Descriptive statistics and relational data analysis techniques were applied in order to anaylze the collected data. The results concluded that the level of digital safety self-efficacy of university students was high, while their online risk-taking propensities were low. Besides, there were statistically significant differences on safety levels of digital applications and commercial risks in terms of gender differences, frequency of internet use, and age groups. Lastly, the results indicated that students' prior online risk-taking propensities predicted their current online risk-taking propensity to some extent.

Keywords: Digital Safety, Online Risks, Online Risk-Taking Propensity, University Students

TEŞEKKÜR

Hayatımın en güzel yıllarını geçirdiğim ve çok güzel ilişkiler kurduğum, doktora eğitimimin büyük bir sürecinde üyesi olduğum Anadolu Üniversitesi'ne veda etmek oldukça zor. Lisansüstü eğitiminde birlikte çalışılabilecek, anlaşılabilecek ve her şeyi paylaşabilecek bir danışmana sahip olmak gerektiğini, deneyimlerimin en değerlisi olarak paylaşmak istiyorum. Doktora eğitimim sürecinde bana güler yüzü, samimiyeti, profesyonelliği, iş ahlakı, disiplini ve azimliliği ile örnek olan, çalışmalar, projeler ve sayamayacağım kadar beceri kazanma konusunda önderlik eden, özellikle dile getiremediğim sıkıntılı zamanlarımda elimden tutan ve doktora tezimde üstün desteğiyle her zaman yanımda olduğunu hissettiren canım tez danışmanım Doç. Dr. Işıl KABAKÇI YURDAKUL'a çok teşekkür ederim. Anadolu Üniversitesi'ndeki tüm sürecimde bana her konuda rehberlik eden, aldığım derslerde ve yaptığım tüm akademik çalışmalarda yardımcı olan, eleştirel ve yaratıcı fikirleriyle ufkumu açan ikinci danışmanım Dr. Öğr. Üyesi Onur DÖNMEZ'e çok teşekkür ederim. Akademik hayatımın şekillenmesinde, duruşları ve çalışmalarıyla her zaman örnek alacağım Prof. Dr. Yavuz AKBULUT ve Doç. Dr. Bahar BARAN'a sonsuz teşekkür ederim. Özellikle tez sürecimde yaşadığım aksaklıklarda yanımda olup bana güvenen ve desteğini gerçekçi bir şekilde gösteren, jürimde yer alıp titiz ve yapıcı dönütleriyle çalışmama değer katan Doç. Dr. Y. Levent ŞAHİN'e teşekkürü bir borç bilirim. Tez izleme jürimde bulunan ve tezimin tüm aşamalarında bana pozitif enerji veren Prof. Dr. Ümit GİRGİN'e teşekkür ederim. Tez savunma jürimde yer alan ve dönütleriyle katkıda bulunan Doç Dr. Ahmet Naci ÇOKLAR'a teşekkür ederim. Tezimin özellikle veri toplama aşamasında desteğini esirgemeyen, Doç. Dr. Elvan GÜNEL, Doç. Dr. Hıdır KARADUMAN, Dr. Öğr. Üyesi Yıldız KURTYILMAZ, Dr. Öğr. Üyesi Bircan ERGÜN BAŞAK, Dr. Öğr. Üyesi M. Bahadır AYAS, Dr. Öğr. Üyesi Ö. Özgür DURSUN'a, Dr. Öğr. Üyesi Mehmet ERSOY, Dr. Öğr. Üyesi İlknur YÜKSEL, Dr. Öğr. Üyesi Gizem UYUMAZ, Arş. Gör. Ümran ALAN, Arş. Gör. Aylin SEVİMEL ŞAHİN, Arş. Gör. Elis SOYLU ve Nilgün EYNEHAN'a teşekkür ederim.

Akademik ve özel hayatımda oldukça değerli olan ve üzerimde emeğini hissettiğim, tezim ve dahi birçok çalışmada yardımlarını esirgemeyen, bana yol gösteren ve yalnız bırakmayan, başarılarıyla gurur duyduğum sevgili Dr. Öğr. Üyesi Fatih YAMAN ve Arş. Gör. Dr. Nihal DULKADİR YAMAN'a teşekkürü bir borç bilirim. Lisansüstü eğitimimim boyunca derslerini aldığım ve deneyimlerinden faydalandığım tüm

hocalarıma üzerimdeki emekleri için teşekkür ederim. Uzun doktora süreci boyunca birlikte ders aldığımız ve çalışmalar yaptığımız iş ve araştırma arkadaşlarıma teşekkürlerimi sunarım. Giresun Üniversite'sinde görev yapmakta olan ve Anadolu Üniversitesi'nden döndükten sonra beni bu zor sürecimde yalnız bırakmayan Doç. Dr. Özlem BAYDAŞ, Dr. Öğr. Üyesi M. Serkan ABDÜSSELAM ve Arş. Gör. Dr. Mithat ÇİÇEK'e teşekkür ederim. Lisansüstü eğitim sürecinde tanıdığım, varlıklarıyla bana huzur veren ve güçlü hissettiren, her ne olursa olsun desteklerini esirgemeyen ve bana katlanan candan dostlarım Dr. Öğr. Üyesi İlknur REİSOĞLU, Arş. Gör. Dr. Ayça ÇEBİ, Arş. Gör. Dr. M. Şahin SOLAK, Arş. Gör. Dr. Şenay OZAN, Arş. Gör. Dr. Tuğba BAHÇEKAPILI, Arş. Gör. Dr. Yasin YALÇIN, Arş. Gör. Eda BAKIR, Arş. Gör. Dr. Hakan İSLAMOĞLU, Arş. Gör. Özge METİN ve Arş. Gör. Yasemin KAHYAOĞLU ERDOĞMUŞ'a kucak dolusu sevgilerimi ve teşekkürlerimi sunarım.

Hayata gözlerimi açtığımdan beri koruyup kollayan, ilk öğretmenlerim olan, emekçi ve azimli, sevgisini ve saygısını hiçbir zaman esirgemeyen benim biricik annem Hacer ÇOLAK ve canım babam Ahmet ÇOLAK'a sonsuz teşekkürlerimi sunarım. Bana sonsuz güvenen ve yaşama sevincimi arttıran evlatlar veren, hayatımdaki en değerlilerim olan kardeşlerim İbrahim ÇOLAK, Arife BOZALİ ve ailelerine çok teşekkür ederim.

Son olarak, kurumsal ve maddi destekleri için Anadolu Üniversitesi Proje Birimi'ne ve TÜBİTAK'a teşekkürlerimi sunarım.

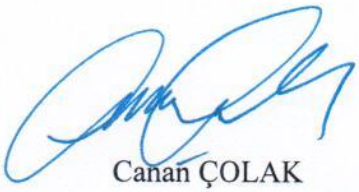
Canan ÇOLAK

Eskişehir 2019

25.06.2019

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Bu doktora tezinin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarda bilimsel etik ilkele ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilemeyen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; bu çalışmanın Anadolu Üniversitesi tarafından kullanılan "bilimsel intihal tespit programıyla" tarandığını ve hiçbir şekilde "intihal içermediğini" beyan ederim. Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara razı olduğumu bildiririm.



Canan ÇOLAK

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

TABLOLAR DİZİNİ

Sayfa

Sayfa

Sayfa

ŞEKİLLER DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

AFA : Açımlayıcı Faktör Analizi
BİT : Bilgi ve İletişim Teknolojileri
BÖTE : Bilgisayar ve Öğretim Teknolojileri Eğitimi
BTK : Bilgi Teknolojileri ve İletişim Kurumu
ÇRAE : Çevrimiçi Risk Alma Eğilimi
DFA : Doğrulayıcı Faktör Analizi
DGÖY : Dijital Güvenlik Öz Yeterliği
MEB : Millî Eğitim Bakanlığı
OAV : Ortalama Açıklanan Varyans
TBA : Temel Bileşenler Analizi
TİB : Telekomünikasyon İletişim Başkanlığı
TUİK : Türkiye İstatistik Kurumu

1. GİRİŞ

İnternet teknolojileri kullanıcılarına, sosyalleşme, eğitim alma, sağlık, bankacılık, gazetecilik, ticaret hizmetlerinden yararlanma, ürün tanıtımı sağlama, çevrimiçi kütüphaneler oluşturma, bilgi depolama ve çeşitli bilgilere erişme gibi birçok olanak sağlamaktadır (Lau ve Yuen, 2016; Vroman, Arthanat ve Lysack, 2015). Bunun yanında kişisel bilginin ifşası, niyetlerinin ne olduğu bilinmeyen bireylerle iletişim kurma, kandırmaca, kötü hizmetle karşılaşma, maddi kayıplara uğrama, uygunsuz içeriklerle karşılaşma, yanlış bilgi yayma ve yanlış bilgiye ulaşma, çeşitli platformlarda sanal topluluklarda küçük düşürülme gibi birçok riski de bünyesinde barındırmaktadır Livingstone, Haddon, Görzig ve Ólafsson, 2011). Son zamanlarda çevrimiçi oyunlar aracılığıyla çocukların savunmasızlıklarını kullanıp, onları sevdikleri ile tehdit eden, psikolojilerinin bozulmasına neden olan hatta intihara sürükleyen, sadece bankacılık işlemlerinde değil, basit kazançlar sağlanabilecek çeşitli hizmetleri kötüye kullanıp kandırmaca ile maddi kazanç sağlamaya çalışan sanal dünyanın kötülerine oldukça fazla rastlanmaktadır (Chang, Miao, Chen, Lee, Chiang ve Chuang, 2016; Sun, Yu, Lin ve Tseng, 2016). Sanal dünyanın kötüleri sadece çocukların savunmasızlığını değil aynı zamanda yetişkinlerin de bilgi ve deneyimsizliklerinden yararlanmaktadırlar. Her geçen gün dijital araçlarda yapılan teknik gelişmeler ve değişimler, onlar aracılığıyla kullanılan uygulamalar ve internetin sunduğu olanaklar artmakta ve buna paralel olarak ne yazık ki bu çevrimiçi ortamlar veya araçlardan doğabilecek tehditler kendilerine yenilerini katmaktadır (Jalali, Kaiser, Siegel ve Madnick, 2019). Dolayısıyla hayatın her alanında vazgeçilmez kolaylıklar sunan bu ağ, araç ve uygulamaların imkanlarını, kullanım oranı her geçen gün arttıkça, çeşitli bilgilere ulaşma, sosyalleşme, kabul görme, etkinlikten faydalanma, hizmetten yararlanma, gündemi takip etme gibi birçok ihtiyaç için çeşitli çevrimiçi riskler göze alınacaktır. Sanal dünyanın tüm bu olanaklarından yararlanırken kullanılabilecek hiçbir güvenlik uygulaması, yazılımı veya donanımı kullanıcılara risksiz bir çevrimiçi ortam sunmamaktadır. Çünkü içerik oluşturma, yayma, iletişim ve etkileşim kurma, çeşitli hizmetlerden yararlanmada kullanıcı faktörü oldukça önemlidir. Fakat var olan ve çeşitleri artan çevrimiçi riskler hakkında ağ, araç ve uygulama kullanıcılarının farkındalıklarının olması ve internet teknolojilerinin nasıl kullanmaları hakkındaki bilgi ve becerilerinin olması oldukça güvenli internet deneyimleri kazanmalarını sağlayacaktır (De Bruijn ve Janssen, 2017).

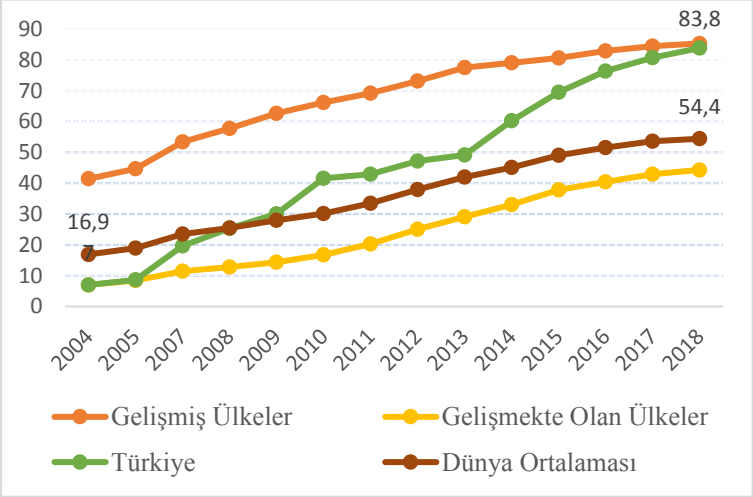
Çevrimiçi riskler ve bu risklere karşı bireylerin sahip olması gereken bilgi ve beceriler sadece teknoloji temelli becerilerden oluşmamaktadır. Bir başka deyişle sadece dijital araçlara virüs programı kurabilmek, işletim sistemlerini güncelleyebilmek, kötü amaçlı yazılımları tarayabilmek veya silebilmekle çevrimiçi riskler veya çevrimiçi riskli davranışlardan kaçınmak sağlanmamaktadır. Bunun yanında karşılaşılan bilgiyi doğrulama, hangi durumlarda ne kadar kişisel bilgi paylaşımının gerektiğini bilme gibi çeşitli önlem ve stratejileri okumaya yarayan medya veya dijital okuryazarlık ve dijital güvenlik becerilerine sahip olmayı da gerektirmektedir (Calvani, Fini, Ranieri ve Picci, 2012).

Sanal ortamlarda karşılaşılan riskler veya çevrimiçi riskli davranışlar incelendiğinde kaba ve rencide edici davranışları barındıran siber zorbalık, kişisel bilgilerin çalınması, dolandırılmak, cinsel sosyalleşme, dijital takip edilme, verilerin silinmesi, bozulması, şiddet veya cinsel içerikli iletilerin paylaşılması veya bu tür paylaşımlara zorlanmak, doğru bilgilerin manipülasyonu ile yanlış bilgilere kitleleri inandırmak, güvenlik, kelime işlemci veya çeşitli hizmetler sunan yazılımları yasal olmayan şekilde edinmek, bilinmeyen sitelerden ürün veya hizmet alım satımı yapmak, güvenilir olmayan e-posta ve eklerinde bulunan talimatlara uymak gibi yelpazenin oldukça geniş olduğu görülmektedir (Byrne, Dvorak, Peters, Ray, Howe ve Sanchez, 2016; Livingstone, Haddon ve Olafson, 2009; Microsoft [Digital Civility Study], 2018; OECD, 2012; Šimandl ve Vaníček, 2017). Bu çevrimiçi riskli davranışların veya risklerin ne olduğu, nereden kaynaklandığını bilmek ve güvenli internet ve internet teknolojilerinin kullanımı için dijital güvenlik becerilerini işe koşmak gerekmektedir. İnternet ve internet teknolojileri kullanım yaşı gün geçtikçe düşmekte, aynı zamanda yetişkinlerin bu teknolojileri kullanım oranları artmaktadır. Artık hareket halinde bile internete bağlı kalınmakta, iletişim ve haberleşmenin yanında sosyal kalma, birçok hizmete erişme ve birçok işlemi gerçekleştirmede internet ve internet teknolojilerine güvenilmektedir (Chauhan ve Panda, 2015). Daha önce de değinildiği gibi tüm bu farkındalık, bilgi ve becerilere sadece çocukların değil tüm yaşlardaki internet kullanıcılarının sahip olması gerekmektedir.

1.1. İnternet Teknolojileri Kullanımı

Bilgi ve iletişim teknolojileri kullanım yaşı giderek düşmekte ve artık çocuklar bile bu teknolojileri kolayca edinip kullanabilmektedir. Ulusal ve uluslararası bazı kuruluşlar

2004-2005 yıllarından 2018'e kadar, hanelerin bilgi ve iletişim teknolojileri kullanımı ve internet erişimleri konusunda yaptıkları araştırmalarla çeşitli istatistiksel sonuçlara ulaşmışlardır. Şekil 1.1'de Türkiye İstatistik Kurumu (TUİK, 2019)'nun bilgi toplumu istatistikleri içinde yer alan hanelerdeki internete erişim oranları ve Uluslararası Telekominikasyon Birimi (International Telecommunucations Union, 2019) tarafından gerçekleştirilen, gelişmiş, gelişmekte ve dünya genelindeki hanelerdeki internet erişim istatistikleri yer almaktadır.



Şekil 1.1. *Hane halkı internete erişim oranı*

Bu oranların 2004 yılındaki verileri kıyaslandığında, Türkiye'deki hane halkı internete erişim oranı %7 iken, dünyadaki diğer ülkelerde bu oranın Türkiye'nin iki katından (%16,9) fazla olduğu görülmektedir. Türkiye'de internete erişim, dünya ortalamasını 2008 yılında yakalarken, 2009-2010 ve 2013-2015 arasında oldukça fazla artış göstermiş ve 2018 yılındaki verilere bakıldığında, Türkiye ile gelişmiş ülkelerde hane halkı internete erişim oranının %83'ün üstüne çıkmıştır. Bu oran dünya ortalamasından (%54,4) oldukça yüksektir. Türkiye'nin internet ve internet teknolojileri hakkında uluslararası ve ulusal kurum ve kuruluşların güncel araştırmaları da mevcuttur. Bilgi Teknolojileri ve İletişim Kurumu (BTK) (2018), Türkiye'de sabit internet abone sayısının 73,8 milyon, mobil internet abone sayısının ise 80,6 milyon olduğunu belirtmiştir. Ayrıca bu araştırmada toplam olarak mobil internet kullanım miktarının ise 846.208 TB olduğu vurgulanmıştır (Statista, 2018). Radyo ve Televizyon Kurulu (RTÜK) (2016)'nun gerçekleştirdiği Medya Okuryazarlığı araştırmasında da benzer sonuçla karşılaşılmaktadır. 8. Sınıf düzeyindeki 871 katılımcının %90,4'ünün internet

kullanıcısı olduğu, internet erişimini mobil araçlarla sağlayanların oranının ise %71,1 olduğu saptanmıştır. İlgili araştırmada katılımcılar internete erişim nedeninin en çok sosyal medya ağlarına katılmak olduğunu belirtmişlerdir. Hootsuite şirketinin güncel istatistikleri incelendiğinde, Türkiye nüfusunun %63'ünün (51 milyon kişi) aktif sosyal medya kullanıcısı olduğu ve günlük olarak ortalama 2 saat 48 dakika bu ortamları kullandıkları saptanmıştır. Ayrıca bu çalışmada mobil araçları olan bireylerin %90'ının mobil internet bağlantısı olduğu da belirtilmiştir (Hootsuite, 2018).

Bireylerin internete erişim oranı ve olanakları hızla artmasının sonucunda, internette hangi aktiviteleri gerçekleştirdikleri, internete erişimde kullanılan teknolojilerin neler olduğu, nereden erişim sağlandığı, kullanım amaçları (Radyo ve Televizyon Üst Kurulu, 2013; 2016), yararları ve beraberinde getirdiği riskli durumları çeşitli kurumsal ve bilimsel araştırmalara konu olmuştur (Kaşıkçı, Çağıltay, Karakuş, Kurşun ve Ogan, 2014). Çocukların ve gençlerin yoğun olarak internet kullanmalarının sebeplerinin araştırıldığı Arslan (2014)'ın çalışmasında; haberlerin takibi, çevrimiçi sohbet, elektronik posta hizmetleri, uzaktan eğitim, oyun oynama gibi çeşitli sosyal içeriklere; hızlı, kolay ulaşabilme ve bu araçları kolaylıkla kişiselleştirebilme imkânlarının olması olarak belirtilmiştir. Bunun yanında Sakarya, Tercan ve Çoklar (2012)'ın çalışmasında da 4. ve 8. sınıf aralığında öğrenim gören öğrencilerin bilgi kaynağı olarak ilk sırada başvurdukları ortamın internet olduğu ve kullanım amaçlarının oyun oynama, haberleşme ve eğlence, film izleme veya müzik dinleme, haberleri takip etme olduğu belirlenmiştir. Özellikle ebeveynleri çalışan bireyler olan çocuklar internet teknolojilerini bir oyun aracı haline getirmişlerdir.

Çocukların dünyasında giderek daha da önemli hale gelen internet teknolojilerinin bilinçsiz kullanımında ise çeşitli fizyolojik, sosyolojik ve psikolojik olarak olumsuz sonuçlar doğabilmektedir (Akbulut, 2013; Arslan Cansever, 2014). Lobe, Livingstone, Ólafsson ve Vodeb, (2011) Avrupa Çevrimiçi Çocuklar Projesi II verilerinden yola çıkarak yaptıkları çalışmada, Türkiye'de internet kullanım oranı ve dolayısıyla çocukların karşılaştıkları çevrimiçi risk oranları diğer Avrupa ülkelerinden daha düşük seviyede olduğu belirtilmiş ve ilgili çalışmada uç değer olarak analize tabi tutulmamıştır. Fakat Şekil 1'deki Türkiye hanedeki internet erişim oranları incelendiğinde, bu oranın en fazla artışı 2013-2016 yılları arasında olduğu görülmektedir. Dolayısıyla internete erişim ve kullanımın hızla arttığı bu ülkede bireylerin çevrimiçi ortamlarda karşılaştıkları riskler ve bu doğrultudaki çevrimiçi riskli davranışlarının da arttığı söylenebilir.

1.2. Çevrimiçi Riskler

OECD (2012) raporuna göre internet, ekonomik ve sosyal etkileşim için gerekli bir alt yapıdır. Tüm kullanıcılar için yararlı yönleri olsa da beraberinde çeşitli riskleri de getirmektedir. Çocuklar internetten eğitim, yaratıcılık ve kendini ifade etme becerisi aynı zamanda kimlik oluşumları ve sosyal becerilerinin gelişiminde oldukça fazla yararlanmaktadırlar. Fakat yetişkinlere oranla risklere karşı daha savunmasızdırlar. İnternet kullanan çocuk sayısı artmakta ve kullanım yaş düzeyi ise azalmaktadır. Bu nedenle de çevrimiçi risklerin belirlenmesi gerekmektedir. Tablo 1.1'de OECD tarafından oluşturulan çevrimiçi risklerin sınıflandırılması sunulmuştur.

Tablo 1.1. *Çocuklar için çevrimiçi riskler*

Çevrimiçi riskler	**İnternet teknolojileri ile ilgili riskler**	İçerik riskleri (Yasak, zararlı içerikler) İletişim riskleri (siber taciz, siber zorbalık, siber sapıklık, yasal olmayan etkileşim, problemli içerik paylaşımı)
	Tüketim ile ilgili riskler	Çevrimiçi pazarlama (Çocuklar için uygun olmayan içerikler, yaş sınırı olması gereken ürünlerin yasal olmayan şekilde satılması, sağlıksız yiyecek ve içecekler) Aşırı harcama Dolandırıcılık (çevrimiçi sahtekarlık, çevrimiçi aldatma, kimlik hırsızlığı)
	Bilgi gizliliği ve güvenliği ile ilgili riskler	Bilgi gizliliği (çocuklar tarafından biriktirilen kişisel bilgiler, aşırı paylaşım, beklenmedik sonuçlar, uzun vadedeki sonuçlar) Bilgi güvenliği (Casus yazılımlar, ticari casuslar, kimlik hırsızları)

OECD (2012), çevrimiçi riskleri genel olarak teknoloji, tüketim ve bilginin gizliliği ve güvenliği ile ilgili riskler olarak kategorize etmiştir. Teknoloji ile ilgili risklerde içerik ve iletişim riskleri yer alırken tüketimle ilgili riskler aşırı harcama, çevrimiçi pazarlama ve dolandırıcılığı kapsamaktadır. Bilginin gizliliği ve güvenliğiyle ilgili riskler ise kişisel bilgilerin aşırı paylaşımı, kimlik hırsızlığı, casus yazılımlar gibi riskleri kapsamaktadır.

Livingstone ve Haddon (2008), çocuklar için çevrimiçi ortamlardaki riskleri dört geniş kategori altında incelemişlerdir. Bunlar; içerik riskleri, etkileşim riskleri, ticari riskler ve gizlilik riskleridir. İçerik riskleri kapsamında, yasal olmayan içeriklerle karşılaşmak, zarar verici içeriklerle karşılaşmak, pornografi, şiddet, ırkçı ve nefret içerikli materyaller ile karşılaşmak, yanlış bilgi, kullanıcılar tarafından oluşturulan problemli içerikler, intihar ve madde kullanımını kapsayan içerikler yer almaktadır. Etkileşim riskleri ise yabancılarla etkileşim kurma ve siber zorbalığı kapsamaktadır. Ticari riskler

arasında; ticari sömürü, yasal dosya indirmeme, kumar yer alırken gizlilik riskleri de kişisel bilgilerin paylaşımı, gizliliğe saldırı, kötü niyetli yazılımlar kullanarak kişisel gizliliği tehdit etmeyi (hacking) kapsamaktadır. Tablo 1.2'de Livingstone, Haddon ve Olafson (2009) tarafından oluşturulan çevrimiçi risk kategorileri ve çocukların bu risklerle karşılaşması durumunda aldıkları rollerin sınıflandırması sunulmuştur.

Tablo 1.2. *Çevrimiçi risk kategorileri ve çocukların bu risklerle karşılaşması durumunda aldıkları roller*

Çocuğun Rolü	Ticari İlgiler	Saldırganlık	Cinsellik	Değerler/İdeolojiler
Alıcı	Reklamcılık, kişisel bilgilerin toplanması	Şiddet unsurları barındıran içerikler	Problemli cinsel öğeler barındıran çevrimiçi içerik	Yanlı bilgi, değerlere hakaret, yönlendirici mesajlar
Etkileşen	İstismar, çocukların takip edilmesi	Taciz edilmek, gizlice izlenmek, siber zorbalığa uğramak	Taciz edilmek, görüşmeye zorlanmak	Yanlış bilgilendirilmek, kendine zarar vermek
Aktör	Yasadışı içeriklere erişim, telif hakların ihlali, kumar siteleri	Siber zorbalık yapmak, küçük düşürmek, kayıt altına almak	Uygunsuz cinsel içerik yayınlamak	Yanlış bilgi yaymak

Hasebrink, Livingstone, Haddon ve Ólafsson, (2009) ise daha kapsamlı bir çalışmada çevrimiçi risk türleri ve çocukların bu risklerle karşılaşması durumunda aldıkları roller dikkate alınarak bir sınıflama yapılmıştır. Tablo 1.2'de gösterilen bu sınıflandırmada; çocukların aldıkları roller, alıcı, etkileşen ve aktör olarak belirlenirken; çevrimiçi risk faktörleri olarak da ticari ilgiler, saldırganlık, cinsellik ve değerler-ideolojiler olarak belirlenmiştir.

18 yaş ve üstü olan ve yetişkin olarak adlandırılan bireylerin de internete erişim oranları, kullandıkları teknoloji türleri (akıllı telefon, tablet, pc vb.) ve internet kullanım süreleri gün geçtikçe artmaktadır (Ofcom, 2017). Sosyal medyalarda var olma, çevrimiçi alışveriş yapma gibi çeşitli dijital becerilerini geliştiren bu bireyler internet aracılığıyla hizmet sunan her kuruluşun önemli birer kullanıcısı haline gelmeye başlamışlardır (Kuoppamäki, Taipale ve Wilska, 2017). Her ne kadar yetişkin bireylerin internet ortamında karşılaştıkları riskli durumlar karşısında bu riskleri yönetebilme becerileri çocuklardan daha fazla olduğu belirtilse de çeşitli çevrimiçi risklerle karşılaşmaktalar veya bu riskli davranışları gerçekleştirmektedirler. Çünkü çevrimiçi riskli durumlarla başa çıkabilme veya bu riskli durumları yönetebilme becerisi sadece zarar-yarar

muhakemesini yapabilme yetisiyle değil, internet kullanım süresi, bu ortamdaki hizmet ve olanaklardan edinilen deneyimler ve kazanımlarla da ilişkilidir (Agosto ve Abbas, 2017; Gamez-Guadix, De Santisteban ve Alcazar, 2017; The Real Cyber Skills Gap, 2017). Bu durumda yetişkin bireylerin de medya kullanma durumları, karşılaştıkları çevrimiçi riskler veya gerçekleştirdikleri riskli çevrimiçi davranışların neler olduğu da önemlidir. Tablo 1.3'te Šimandl ve Vaníček (2017)'in çevrimiçi riskler ve kaynakları sınıflandırması yer almaktadır.

Tablo 1.3. *Çevrimiçi riskler ve kaynakları*

Çevrimiçi Riskler	**Kişilerarası ilişkilerden kaynaklanan riskler**	Stalklamak
		Cinsel paylaşımlar
		Zorbalık
		Trollenmek
	Teknik güvenlik becerilerinden kaynaklanan riskler	Şifre işlemleri
		Veri yedekleme
		Kişisel bilgi paylaşımı

Byrne, Dvorak, Peters, Ray, Howe ve Sanchez, (2016) çalışmasında, 19-68 yaş aralığındaki bireylere internette gerçekleştirdikleri eylemleri ve bu eylemlerde neden bulunduklarını araştırmışlardır. Tablo 1.3'te sıklıkla gerçekleştirilen, bankacılık işlemleri, e-posta kontrolleri, fotoğraf aratma gibi 35 internet eylemi listelenmiştir. Daha sonra bu listedeki eylemlerin ne derece riskli olarak algıladıkları belirlenmiştir. Tablo 1.4'te Byrne, vd., (2016)'nin yetişkin bireylerin internette sıklıkla gerçekleştirdikleri eylemler ve bu eylemleri kategorize ettikleri risk grupları sunulmuştur.

Tablo 1.4. *İnternette sıklıkla gerçekleştirilen eylemler ve bu eylemlerin risk grupları*

Bilgi riskleri	Haber makalelerini okuma
	Web gezinimi
	Bilgi arama
	Sağlık sitelerinden bilgi edinme
	Blog haberlerini takip etme
	Gezinme, tıklama
	Ürün arama
	Çevrimiçi videolara erişme
Sosyal riskler	Resim indirme
	Fotoğraf yükleme
	Fotoğraf arama
	Skype, Messenger kullanma
	Youtube'a yükleme yapma-İzleme
	Sosyal medya kullanma

Tablo 1.4. (Devam) *İnternette sıklıkla gerçekleştirilen eylemler ve bu eylemlerin risk grupları*

Finans riskleri	Bilinen bir siteden alışveriş yapma
	Bankacılık işlemleri gerçekleştirme
	Çevrimiçi ticaret
	Bilinmeyen sitelerden alışveriş yapma
	İkinci el sitelerde satış yapma
Çeşitli riskler	Ses
	Gezi siteler aracılığıyla işlem yapma
	Metin indirme
	Oyun indirme
	Paylaşımlı eğlencelere katılma
Uygulama riskleri	Ekli dosyaları açma
	E-postalardaki bağlantılara tıklama
	Verimli şablonlar
Oyun riskleri	Başkalarıyla çevrimiçi oyun oynama
	Etkileşimli olmayan eğlencelere katılma
	Çevrimiçi kumar oynama
	Tek kullanıcılı oyunlar oynama
E-posta riskleri	Ekleri açma
	E-postaları açma

Çalışmada ortaya çıkan risk grupları; bilgi riskleri, sosyal riskler, finansal riskler, çeşitli riskler (Paylaşım riskleri), uygulama riskleri, oyun riskleri ve e-posta riskleridir. Çalışmada her ne kadar yetişkin bireylerin internet kullanımlarındaki sıklıkla gerçekleştirdikleri eylemler üzerinde durulsa da bu eylemler hakkındaki risk algıları da incelenmiştir. Risk algılarını gruplamak için de bir çerçeve oluşturmuşlardır.

Šimandl ve Vaníček (2017)'in elektronik güvenliği ele aldıkları ve katılımcılarının yetişkinler olduğu araştırmada, karşılaşılan çevrimiçi risklerin kaynaklarından yola çıkılarak bir sınıflandırma yapıldığı Tablo 1.3'te görülmektedir. Burada kişilerarası ilişkilerden ve teknik güvenlik becerilerden kaynaklanan çevrimiçi riskler olduğu vurgulanmıştır. Tablo 1.5'te Microsoft [Digital Civility Study] (2018)'in çevrimiçi riskler çerçevesi yer almaktadır.

Tablo 1.5. *Microsoft çevrimiçi riskler çerçevesi*

Davranışsal	**İtibarsal**	**Cinsel**	**Kişisel/Zoraki**
Tehdit etmek	Sanal ortamda kişisel bilgiye ulaşılması	İstenmeyen cinsel içerikli iletiler almak	İstenmeyen iletişim
Trollenmek	Kişisel itibara zarar verme	Uygunsuz cinsel sosyalleşme	Nefret söylemi
Çevrimiçi taciz	İş itibarına zarar verme	İstenmeyen cinsel içerikli iletiler göndermek	Ayrımcılık

Tablo 1.5. (Devam) *Microsoft çevrimiçi riskler çerçevesi*

Davranışsal	İtibarsal	Cinsel	Kişisel/Zoraki
Siber zorbalık		Seksüel zorlama	Terör
Aşağılamak – ezmek		İntikam amaçlı cinsel içerikler	Kadın düşmanlığı
Mikro saldırganlıklar			Aldatmak/Dolandırmak /Oyuna getirmek

13-17 ve 18-74 yaş aralığındaki bireylerin katılımıyla gerçekleştirilmiş Dijital Medeniyet Çalışmasında (Digital Civility Study) çevrimiçi ortamlarda karşılaşılan yirmi birbirinden farklı çevrimiçi riskin olduğu vurgulanmıştır. Tablo 1.5'te belirtilen bu riskler davranışsal, itibarsal, cinsel ve kişisel/zoraki olarak sınıflandırılmıştır. Bu çevrimiçi riskli durumlar incelendiğinde, kişisel ve iş itibarına zarar verme, cinsel sosyalleşme ve mikro saldırganlıklar ile ilgili çevrimiçi riskler veya riskli davranışlar konularında çocukların karşılaştıkları çevrimiçi risklerden farklılaşmaktadır.

Çevrimiçi risklerin ele alındığı çalışmalarda öncelikle çocuklar için çevrimiçi risk çerçeveleri oluşturulmuştur. Fakat son yıllardaki çalışmalara bakıldığında, internet kullanan her yaştaki birey için çeşitli risklerin olduğu ortaya çıkmıştır. Çevrimiçi riskler ele alınırken riskler karşısında bireylerin aldıkları roller, risklerin kaynakları ya da risklere neden olabilecek benzer internet eylemlerinin gruplanması temel alınarak çeşitli sınıflandırmalar yapılmıştır. Bu sınıflandırmalar hem çevrimiçi risklerin çeşitliliğinin artması hem de bilimsel araştırmaların ele aldıkları katılımcılar ve incelenen değişkenler bağlamında değişik bakış açıları sunması açısından oldukça önemlidir. Ele alınan çevrimiçi riskler çerçevelerinde, çocuklar için belirlenen çevrimiçi risklerden farklı olarak yetişkinlerin, şifre işlemleri, veri yedekleme gibi teknik güvenlik becerilerinden, finansal işlemler, iş itibarının zedelenmesi gibi çocuk bireylerin henüz içinde bulunmadıkları ya da edinmedikleri kazanımlar konularında risk aldıkları veya maruz kaldıkları dikkat çekmektedir.

1.3. Dijital Güvenlik

Alışveriş, fatura ödeme, bir etkinliğe kayıt olma ya da sosyal kalma, hatta iş hayatını sürdürebilme gibi birçok ihtiyaç için çevrimiçi uygulamalar ve dijital araçlar kullanılmaktadır. Dolayısıyla tüm bu ihtiyaçların karşılanması için, internetten erişilen çeşitli platformlara güvenilmektedir (Chauhan ve Panda, 2015). Fiziksel dünyada da olduğu gibi sanal dünyada tüm bu işlemleri gerçekleştirmede güvenlik sorunları

mevcuttur. Halamka (2017), dijital güvenliği, kişinin mahremiyeti ve çeşitli verilerinin bütünlüğünü koruma altına alabilecek politikalar ve teknik korumaların işe koşulmasıyla sağlanabileceğini belirtmiştir. Dijital güvenliği sağlamak sadece arama motoru ayarlarını yapılandırmak, güvenli uygulamalar kullanmak, güvenilir siteleri ziyaret etmek, örneğin güncellenmiş virüs programı ya da güvenlik duvarı gibi yazılımları kullanmakla sağlanamamaktadır. Dijital güvenlik, kullanıcıların verilerinin güvenliğini de kapsamaktadır. Dijital güvenlikle aslında, internet kullanıcılarının çevrimiçi ortamlarda gelebilecek tehditler hakkında farkındalıklarının olması ve güvenli bir şekilde internet hizmetinden yararlanabilmeleri için bu tehditler karşısında ne yapacağını bilmeleri gerektiği ifade edilmektedir (Baker, 2015; Chauhan ve Panda, 2015; Halamka, 2017; Jeske ve Van Schaik, 2017).

1.3.1. Dijital güvenlik tehditleri

Sıklıkla karşılaşılan dijital tehditlerin sınıflandırmaları mevcuttur. Chauhan ve Panda (2015), kötü amaçlı yazılımlar (Malwares), kimlik avcılığı (Phishing), çevrimiçi dolandırıcılık (Online scams and frauds), saldırı girişimleri (Hacking attempts), güçsüz şifreler (Weak password), omuz sörfü (Shoulder surfing), sosyal mühendislik (Social engineering) saldırıları olarak sıklıkla karşılaşılan dijital tehditleri sınıflandırmıştır. İlgili sınıflandırmada kötü amaçlı yazılımlar altında; virüsler (Virus), Truva atları (Trojan), verileri bloke eden yazılımlar (Ransomware), kullanıcı adı ve şifreleri kaydedici programların (Keylogger) oluşturduğu yazılımlar ele alınmıştır. Jeske ve Schaik (2017), Garg ve Camp, (2012), Huang, Rau ve Salvendy (2010) çalışmalarında listelenen ve Schaik, Jeske, Onibokun, Coventry, Jansen ve Kusev (2017) çalışmasında sınıflandırılan dijital tehditler; kimlikle ilgili tehlikeler, izleme (takip etme) tehlikeleri, yazılımla ilgili tehlikeler, çevrimiçi sosyal tehlikelerdir. Kimlikle ilgili tehlikeler arasında, kimlik avcılığı (Phishing), kimlik hırsızlığı (Idendity theft on the Internet), izleme ile ilgili olarak çevrimiçi izleme (Internet surveillance), yazılımla ilgili tehlikeler; virüs (Virus), çerezler (Cookie), casus yazılımlar (Spyware), şifreleri kaydeden programlar (Keylogger), Truva atları (Torjan), zararlı yazılımlar barındıran özel ağlar (Botnet), sahte antivirüs programları (Rogueware), yazılım açıklarını kullanan zararlı yazılımlar (Zero-day attack), e mail toplayıcı yazılımlar (e-mail harvesting), çevrimiçi sosyal tehlikeler arasında da; sanal izlenme (Virtual stalking), siber zorbalık (cyber-bullying), sosyal mühendislik (social engineering), sahte duygusal ilişki kurma eylemleri (Catfishing) yer

almıştır. Kötü amaçlı yazılımlar (Malwares), genellikle yetişkin içerikli siteler gibi erişimi kısıtlanmış, ücretsiz müzik ya da yazılım indirmeyi sağlayan sitelerden dijital araçlarımıza bulaşan ve dijital ortamlarımızda depoladığımız verilerimizi kullanmamızı engelleyen ya da bu verilere erişen yazılımlardır. Aşağıda kötü amaçlı yazılım türleri maddeler halinde belirtilmiştir.

- Virüsler (Virus), işletim sistemine, depolanan verilere bulaşan ve bu sistem ve verilerin kullanılmasını bozan zararlı yazılımdır. Verilerin bulunduğu belleklerin bozulmasına, ilgili verilerin silinmesine veya kontrolsüz bir şekilde kopyalanmasına sebebiyet verir.
- Truva atları (Trojan); genellikle ücretsiz bir indirme işlemiyle birlikte dijital aracınızın işletim sistemine bulaşan yazılımlardır.
- Verileri bloke eden yazılımlar (Ransomware) ise, dijital aracınızdaki verileri veya sistem dosyalarını bloke ederek, bu veri veya kaynakları kullanabilmek için fidye talep eden kötü amaçlı yazılımlardır.
- Kullanıcı adı ve şifreleri kaydedici programlar (Keylogger); dijital aracınıza bulaştığı andan itibaren tüm hareketlerinizi kaydeden program parçalarıdır. Bu tür kötü amaçlı yazılım kişisel bilgilerin kaydedilmesi ve saldırganlara gönderilmesine sebebiyet vermektedir.
- Kimlik avcılığı (Phishing); Saldırganın, kullanıcının giriş yapması gereken orijinal site sayfasına oldukça benzeyen bir sayfa içeren sahte bir bağlantı göndererek kullanıcıyı kandıracağı basit fakat hala popüler olan bir saldırıdır.
- Çevrimiçi dolandırıcılık (Online scams and frauds); genellikle spam postaları ile bulaşan, kullanıcı bilgilerini kopyalayıp, sanki tanıdığınız kişilerden gelen yardım çağrıları ile maddi kazanç sağlamayı amaçlayan yazılımlardır.
- Çerezler (Cookies) ise, kullanıcıların dijital araçlarında depolanan ve gezindikleri web ortamları ve bu ortamlarda kullandıkları veriler hakkında bilgiler içermektedir. Dolayısıyla çerezlere erişen saldırganlar kullanıcı gezinim verilerini ele geçirmektedir.
- Zararlı yazılımlar barındıran özel ağlar (Botnet), bir dizi özel bilgisayarlardaki zararlı yazılımla dijital araçları sahiplerinin bilgileri dışında tüm veri transferlerini bağlı oldukları ağdaki diğer tüm bilgisayarlara gönderen tehdit türüdür.
- Oluşturulan yeni bir yazılımın açıklarını, o yazılımı oluşturanlardan önce bulmak için kullanan zararlı yazılımlar (Zero-day attack) da önemli bir dijital tehdittir.

- E-posta adresi toplayıcı yazılımlar (e-mail harvesting) ise birçok e posta adresini kişilerin bilgisi olmadan elde eden ve bu kişilere spam dosyaları göndermek amacıyla kullanan yazılımlardır.

Saldırı girişimleri (Hacking attempts); genellikle yaygın kullanılan masaüstü uygulamalar ya da tarayıcı eklentileriyle bulaşan, kullanıcıların tarayıcılarında gerçekleştirdikleri tüm eylemleri toplayan bilgisayar korsanı saldırısı olarak nitelendirilmektedir. Aşağıda saldırı girişim türleri maddeler halinde belirtilmiştir.

- Güçsüz şifreler (Weak password), kullanıcı kolaylığı için birçok uygulama parolanın karmaşıklığını zorlamamaktadır. Böylece kullanıcılar tahmin edilmesi kolay olan sıralı numaralar, doğum tarihleri gibi şifreler kullanmaktadırlar. Bu durum ilgili kullanıcının verilerini veya kullandığı hesabı saldırılara açık hale getirmektedir.
- Omuz sörfü (Shoulder surfing), aynı ortamda bulunulan iş arkadaşları, sınıf arkadaşları ya da akrabaların, bireysel hesap bilgilerinizi kullanmak istemesiyle gerçekleşen, şifre veya kullanıcı adı gibi bilgilerinizi ilgili dijital platformu kullanmak için tuşlarken görmesi ve daha sonra kötü amaçla kullanmasıyla gerçekleşir.
- Sosyal mühendislik (Social engineering), saldırı türünde ise saldırgan öncelikle kurbanın güvenini kazanır ve zamanla bilgilerini toplar. Ardından daha önce bahsedilen dijital tehditlerden birini kullanarak kurbanın verilerini ya da sistem dosyalarını ele geçirir.
- Sanal izlenme (Virtual stalking), çeşitli bilgi ve iletişim teknolojilerini, dijital izlerini tekrarlı bir şekilde takip ederek başkası hakkında bilgi edinme ve ilgili kişiye zarar vermek amacıyla kullanmaya sebebiyet veren bir saldırı türüdür.
- Siber zorbalık (Cyber-bullying), özellikle internet üzerinden diğer bireylere zarar vermek veya taciz etmek için bilgi ve iletişim teknolojilerinin bilinçli, tekrar eden ve düşmanca kullanılmasıyla gerçekleşen bir saldırı türüdür.
- Sahte duygusal ilişki kurma eylemleri (Catfishing) ise, sahte bir sosyal medya profili ile başka birisi gibi davranarak çevrimiçi romantik bir ilişki kurmayı ve ilişki kurulan bireyin duygusal olarak zarar görmesini amaçlayan saldırı türüdür.

Tüm bu kötü amaçlı yazılımlar ya da saldırganlık türleriyle dijital teknolojileri kullanan bireylerin kişisel bilgileri ve verilerine erişip kötüye kullanma amacı güdülmektedir. Dolayısıyla kullanıcıların her gün yenisi eklenen bu tehditler (Baker,

2015; Huang, Rau ve Salvendy, 2007) karşısında hayatın ayrılmaz bir parçası olan interneti güvenli kullanabilmeleri için çeşitli bilgi ve becerilere sahip olmaları ve bu becerileri işe koşmaları gerekmektedir.

1.3.2. Dijital güvenlik becerileri

Bilgi ve iletişim teknolojileri kullanıcılarının kötü amaçlı yazılımlarla veya çevrimiçi saldırılarla baş edebilmeleri için daha önce de vurgulanan bu dijital tehditler hakkında farkındalıklarının olması ve dijital iyi oluşlarını sağlamaları gerekmektedir. Bu doğrultuda kötü amaçlı yazılımlarla veya çevrimiçi saldırılarla baş edecek çeşitli teknik uygulamalar, kullanıcıların almaları gereken önlemler ya da kullanmaları gereken stratejiler bulunmaktadır (Sonck, Livingstone, Kuiper ve De Haan, 2011). Her gün yenisi eklenen bu dijital tehditler karşısında takipte olmaları ve bu tehditlere karşı alınabilecek önlemleri, kullanılacak stratejileri öğrenip işe koşmalıdırlar. Öncelikle dijital güvenliğin sağlanması konusunda kötü amaçlı yazılımlarla baş edebilmek için bilgisayarlar ve akıllı telefonların işletim sistemlerini ve kullanıcı verilerini koruyabilecek çeşitli yazılımlar ya da uygulamalar bulunmaktadır. Bunlar arasında erişim kontrolü yapan uygulamalar, antivirüs programları, hesaplara erişim denetimi yapan uygulamalar, kimlik doğrulaması yapan uygulamalar, yedekleme ve yeniden yükleme uygulamaları, biyolojik özelliklerle doğrulama yapan uygulamalar, içerik filtreleme uygulamaları, veri tabanı güvenliğini sağlayıcı uygulamalar, kopyalamaya karşı koruma uygulamaları, ağ üzerinden koruma uygulamaları, sistem kurtarma uygulamaları, e-posta güvenliği, elektronik ticaret güvenliğini sağlayıcı uygulamalar, kurumsal güvenlik yönetimi sağlayan uygulamalar, güvenlik duvarları, erişim güvenliği uygulamaları, izinsiz giriş tespit edici uygulamalar, bellek koruyucu uygulamalar, akıllı kartlar, tek oturum açıcı uygulamalar, sanal özel ağlar, güvenlik açığını tarayıcı yazılımlar yer almaktadır (Vacca, 2013).

Antivirüs, filtreleme gibi yazılım veya uygulamaların güncelliğine oldukça fazla dikkat edilmelidir. Çünkü kötü amaçlı yazılımlar her gün kendilerini yenilemektedirler. Dolayısıyla dijital araçlarında antivirüs, güvenlik duvarı gibi çeşitli güvenlik yazılımı veya uygulamaları kullananların bu programları güncelleyebilmeleri, dijital araçlarında herhangi bir güvenlik sorunu yaratabilecek virüs, Truva atı gibi kötü amaçlı yazılım olup olmadığını kontrol edebilmelidirler. Dijital araçlardaki işletim sistemleri veya bu işletim sistemleri üzerinde çalışan uygulamaların güvenlik açıkları bulunabilmektedir. Bu

açıkların kapatılması, dolayısıyla işletim sistemleri ve kullanılan diğer paket programların güncellenmesi dijital güvenlik için diğer bir gerekliliktir.

Kimlik hırsızlığı ya da çevrimiçi dolandırıcılıkla ilgili yapılan saldırılar genellikle güvenilen siteler veya bilinen e-posta hesaplarıyla spam olarak elektronik hesaplara, oradan da dijital araçlardaki kullanıcı verilerine veya sistem dosyalarına bulaşmaktadır (Chauhan ve Panda, 2015). Bu tür durumlarla karşılaşmamak için emin olunmayan, şüpheli bilgiler ve ekler içeren bağlantıları ayırt edebilmek ve bu tür bağlantılara bireysel dijital hesapları ya da dijital teknolojileri kullanarak erişmemek gerekmektedir. Ayrıca güvenli sitelerin sağladığı hizmetlerden yararlanıldığına emin olunmalıdır. Web tarayıcıları üzerinde kullanılan güvenlik modülleri de dijital güvenliği sağlamada önemlidir. Birçok internet kullanıcılarının ilgili web sitelerinin ne kadar güvenilir bulduklarını belirttikleri ve oyladıkları bir uygulama kullanarak ilgili içeriğin gözden geçirilmesi ve web'in daha güvenilir bir yer haline getirilmesi sağlanabilir. Kullanıcı ve server arasında veri alışverişini daha güvenilir hale getiren "https" protokolü desteğine sahip hizmetlerin tercih edilmesi bir başka dijital güvenlik önlemidir. Buna ek olarak web adreslerinin arama motorunun adres çubuğuna doğrudan yazılması ve yönlendirici bağlantılar tercih edilmemesi de bir diğer güvenlik önlemidir. Üyelik için başvurulacak web sitelerine gerektiğinden fazla bilgi ve kişisel bilgilerin sorgulandığı e-posta veya mesajlara yanıt verilmemelidir. Çevrimiçi alışverişlerde, ödeme kartı bilgilerini güvenlik altına alan hizmetler kullanılmalı, mümkünse düşük limitli ve tek bir ödeme kartı bilgisi verilmelidir. Bunun yanında çevrimiçi alışverişlerde sanal kart uygulaması, ödeme güvenliği sağlayıcı eklentiler kullanımı da oldukça önemlidir.

Kullanıcıların çevrimiçi saldırılar karşısında kendi elektronik hesap bilgileri ve dijital araçlarındaki verilerinin korunması için çeşitli küçük büyük harfler, rakamlar ve özel karakterlerin kombinasyonuyla oluşturdukları tahmin edilmesi mümkün olmayan güçlü şifreler kullanmaları da önemli bir dijital güvenliği sağlama stratejilerinden biridir. Genel olarak güçlü bir şifrenin sekiz karakterden fazla, büyük küçük harf, rakam ve özel karakterler içermesi gerekmektedir. Buna ek olarak web tarayıcılarında bulunan şifremi hatırla seçeneğini işaretlenmemeli, her 60-90 günde bir şifre değiştirme işlemi yapılmalı ve her e-hesabınızda veya dijital araçlarınızda farklı ve güçlü şifreler kullanılmalıdır. Ayrıca kullanıcıların verilerini depolandıkları dijital araçlar, şifreleme yazılımı kullanarak da korunabilir (Hadlington, 2017). Sosyal mühendislik karşısında hangi bilgilerin hassas olduğunun bilinmesi ve kullanıcı adı, şifre gibi özel bilgilerin, iş

arkadaşı, sınıf arkadaşı veya akraba gibi başka bireylere verilmemesi alınabilecek güvenlik önlemleri arasındadır. Ayrıca başka dijital araçlarda hangi kötü amaçlı yazılımın olup olmadığının bilinmemesi sebebiyle, bu araçlarda e-posta, site üyelikleri vb. hesap bilgileri kullanılmamalıdır. Kullanıldığında ise ilgili dijital araçtaki izlerin silinmesi, arama motoru gizlilik ve güvenlik ayarlarını yapılandırılması, gizli arama seçeneğinin kullanılması gerekmektedir. Sahte bir hesapla başkasıymış gibi görünen, güven oluşturup, duygusal bir ilişki kurmaya çalışan ya da sosyal medyalar, çevrimiçi sohbet ortamları aracılığıyla sanal olarak takip ederek, kişisel bilgilerin çalınmasına ve duygusal olarak zarar vermeyi amaçlayan tehditler karşısında ise çevrimiçi ortamlarda özel iletişim ve etkileşim kurmamaya, herhangi bir hassas bilginin paylaşılmamasına dikkat edilmelidir (Akcil, Altinay ve Altinay, 2016; Rathore, Sharma, Loia, Jeong ve Park, 2017).

Çevrimiçi saldırıların nihai amacı aslında kullanıcıların önemli bilgi ve verilerine ulaşmak, duygularını incitmek, maddi birikimlerini çalmak veya iyi oluşlarını engellemektir. Sanal dünya güvenlik önlemi alınması gereken bir ortamdır. Saldırganlar için güvenlik zincirinde en zayıf halkası insanlardır. Bu anlamda saldırıları, saldırganlık yöntemlerini anlamak ve bu doğrultuda dijital hayatı daha güvenli hale getirecek doğru stratejileri kullanmak ve önlemleri almak gerekmektedir (Chauhan ve Panda, 2015).

1.4. Çevrimiçi Risk Alma ve Dijital Güvenlik Öz Yeterliği ile İlgili Değişkenler

Alanyazında çevrimiçi riskler ve dijital güvenlik konuları çeşitli değişkenler açısından ele alınmıştır. Bunlar arasında; cinsiyet, yaş, eğitim seviyesi, internet kullanım sıklığı, internet kullanım süresi gibi demografik özelliklerin yanında, kişilik özellikleri, ebeveyn arabuluculuğu, sanal ortamlara duyulan güven, dijital okuryazarlık becerisi, dijital güvenlik becerileri, risklerle başa çıkma stratejileri, risk algısı, algılanan yarar, risk eğilimi, davranış değerlendirme yolu gibi değişkenler yer almaktadır. Derlenen bu değişkenler doğrultusunda araştırmada da ele alınan cinsiyet, yaş, bilim dalı, internet kullanım sıklığı, dijital güvenlik öz yeterliği ve çevrimiçi risk alma eğilimi değişkenleri ele alınmıştır.

Cinsiyet, özellikle çevrimiçi riskler ve dijital güvenliği sağlama konularında birçok çalışmada incelenmiştir. Erkeklerin kadınlara göre karşılaşılan uygunsuz içerikler gibi riskler karşısında daha aktif başa çıkma stratejisi kullanmaları (Soldatova ve Zotova, 2013), kadınların siber zorbalık ve cinsel saldırganlık riskleri karşısında kurban

durumuna düşmeleri (Pujazon-Zazik, Manasse ve Orrell-Valente, 2012), erkeklerin ise siber saldırganlık davranışlarını kadınlara göre daha fazla göstermeleri (Baştürk Akça, Sayımer ve Ergül, 2015) cinsiyetin çevrimiçi riskli davranışlar çerçevesinde ele alınması gereken önemli bir değişken olduğunu kanıtlamaktadır. Bununla birlikte dijital güvenliği sağlama konusunda da benzer bir durum söz konusudur. Çünkü kadınlar, erkeklerden daha az güvenlik tehditlerini önleyecek farkındalıklara sahip olduklarını, hatta daha zayıf güvenlik davranışı gösterme niyetleri olduğunu belirtmektedirler (Gratian, Bandi, Cukier, Dykstra ve Ginther, 2018). Özellikle yeni yaygınlaşan çevrimiçi riskler karşısında güvenlik önlemi alma konusunda erkeklerin kadınlara göre daha yeterli olduğu da dikkat çekmektedir (Sun, Yu, Lin ve Tseng, 2016).

Çevrimiçi riskler konusunda, **yaş** değişkeniyle ilişkili olan özellikle bireylerin gelişim dönemleri bağlamında ayrı ayrı dönemlere ilişkin gelişen bir literatür vardır. Yani çocuklarda yarar-zarar mekanizmalarının henüz gelişmemiş olması ve bu nedenle karşılaşılan çevrimiçi risklerin onlara faydalı mı zararlı mı olduğunu bilememeleri, ergen bireylerin kendilerine olan ekstra güvenleri ve her şeyin üstesinden gelebilme hisleri, bir başka deyişle bir çevrimiçi riskli davranışı bana bir şey olmaz düşüncesiyle gerçekleştirmeleri, yetişkenlerin gelişmiş muhakeme yetenekleri gerçek hayattaki risk alma davranışlarıyla ilişkili olduğu gibi çevrimiçi riskli davranışlarla da ilişkili olduğu ortaya koyulmuştur. Yetişkinlerin internette gezinirken daha güvenli hareket ettikleri (Van Bavel, Rodríguez-Priego, Vila ve Briggs, 2019), buna karşın da dijital güvenlik tehditleri ile başa çıkabilecek farkındalık ve deneyimlerinin azlığı (Jiang, Tsai, Cotten, Rifon, LaRose ve Alhabash, 2016) çeşitli araştırma sonuçları arasında yer almaktadır. Bu nedenle bireylerin içinde bulundukları dönemleri ve dolayısıyla yaş değişkenini çevrimiçi risk alma ve dijital güvenliği sağlama konularında irdelemek oldukça önemlidir.

Öz yeterlik, bireylerin çeşitli performansları başarma durumlarına ilişkin yargısı olarak tanımlanmaktadır (Bandura, 1982). Pajares (2002), belirli konudaki performansı göstermede istenilen başarıya ulaşılmadığı sürece o performansı göstermeye teşebbüs etmenin veya o konuda zorluklarla karşılaşıldığında, dayanma gayreti gösterilmesinin beklenilmemesi gerektiğini ifade etmiştir. Çünkü öz yeterlik, bireylerin yeterli olduklarını hissettikleri işlere girişimde bulunmaları, zorluklar karsısında kolayca vazgeçmemeleri ve davranışı tamamlamalarında etkilidir (Bandura, 1986). Öz yeterlik aynı zamanda Rogers (1983)'ın Korunma Motivasyonu Teorisi (Protection Motivation Theory) içerisinde ele alınan, bireyin bir tehditle karşılaşması durumunda, tehditi en aza indirmeye

yardımcı olabilecek davranışlarda bulunulmasına teşvik edici bilişsel süreçlerden birisi olarak da tanımlanmıştır (Doane, Boothe, Pearson ve Kelley, 2016). Korunma Motivasyonu Teorisi'ndeki öz-yeterlik kavramıyla, bireyin belirli bir güvenlik davranışını yerine getirmedeki beceri ve yetenekleri ile ilgili algısına odaklanılmaktadır (Ifinedo, 2012). Genellikle davranış kuramları ile birlikte ele alınan öz yeterlik, bilgisayarlar ve mobil cihazlarda bilgi güvenliğini sağlama konusundaki bireylerin niyetlerinin en güçlü tahmin edicisi (Thompson, McGill ve Wang, 2017; Verkijika, 2018) ve bilgi güvenliğini sağlama konusunda olumlu etkiye sahip olduğu bulunmuştur (Doane vd., 2016; Ifinedo, 2012; Sun, Yu, Lin ve Tseng, 2016; Verkijika, 2018). Dolayısıyla dijital güvenliği sağlama konusunda önemli bir değişken olarak ele alınmıştır.

Risk, önemli veya hayal kırıklığına uğratan sonuçlarının gerçekleşip gerçekleşmeyeceği konusundaki belirsizlik olarak tanımlanan kararların bir özelliğidir (Sitkin ve Pablo, 1992). **Risk eğilimi**, Sitkin ve Pablo (1992)'nun "karar vercinin risk alma ya da önleme eğilimi" tanımından yola çıkarak "bireylerin farklı tür alanlarda riskli davranış sıklıkları" olarak tanımlanmıştır (Nicholson, Soane, Fenton-O'Creevy ve Willman, 2005). Bunun yanında Sitkin ve Weingart (1995)'in riskli karar verme davranışının belirleyicilerini araştırdığı çalışmasında geçmişteki ilgili davranışların sonuçlarının, riskli karar verme davranışının belirleyicilerinden biri olduğunu göstermiştir. Hatta riskli karar verme davranışının belirleyicilerini gösterdikleri modelde, geçmişin risk eğilimini, risk eğiliminin risk algısını, risk algısının da riskli karar verme davranışını etkilediğini öne sürmüşlerdir. Bunun yanında, Weber, Blais ve Betz (2002), risk alma davranışının içerik yani alan temelli olarak gerçekleştirildiğini belirtmiştir. Örneğin finansal alanda riskli kararlar veren kişiler sosyal konularda riskli kararlar vermeyebileceklerini belirtmişlerdir. Bu çalışmada da çevrimiçi risk alma eğilimi konusunda geliştirilen ölçme aracında bu ortamdaki risk türlerinin de alanlara ayrılabileceği ön görülmüştür. Sitkin ve Weingart (1995) risk eğiliminin, bireylerin riskler konusunda geçmişteki deneyimlerinden de etkilendiğini, dolayısıyla risk eğilimi üzerinde zaman etkisinin olduğunu vurgulamışlardır. Buna ek olarak risk algısı ve risk eğiliminin riskli davranışın karakteristik bir özelliği olduğunu belirtmişlerdir. Dolayısıyla bu çalışmada, Nicholson, Soane, Fenton-O'Creevy ve Willman (2005)'ın kullandıkları gerçek hayattaki riskli alanlara ilişkin hazırlanmış "Risk Alma Çerçevesi" ölçme aracındaki gibi geçmişteki çevrimiçi riskli karar gösterme sıklığı ile şimdiki çevrimiçi risk alma eğilimleri incelenmiştir.

1.5. Amaç

Bu çalışmanın amacı, üniversite öğrencilerinin çevrimiçi risk alma eğilimlerinin dijital güvenlik öz yeterlikleri tarafından yordanma durumu ile çevrimiçi risk alma eğilimleri ve dijital güvenlik öz yeterliklerinin farklı demografik özellikleri açısından incelenmesidir. Çalışmanın genel amacı doğrultusunda aşağıda yer alan alt problemlere yanıt aranmıştır:

1. Üniversite öğrencilerinin dijital güvenlik öz yeterlikleri, şimdiki çevrimiçi risk alma eğilimleri
    a. Cinsiyete,
    b. Yaş gruplarına,
    c. Öğrenim gördükleri bilim dallarına,
    d. İnternet kullanım sıklıklarına göre farklılaşmakta mıdır?
2. Üniversite öğrencilerinin geçmişteki çevrimiçi risk alma eğilimleri cinsiyete göre farklılaşmakta mıdır?
3. Üniversite öğrencilerinin dijital güvenlik öz yeterlikleri, şimdiki çevrimiçi risk alma eğilimleri ve geçmişteki çevrimiçi risk alma eğilimleri arasında ilişki var mıdır?
4. Üniversite öğrencilerinin geçmişteki çevrimiçi risk alma eğilimleri, şimdiki çevrimiçi risk alma eğilimlerini yordamakta mıdır?

1.6. Önem

İnternet, bireyler için önemli bir etkileşim ortamıdır. İnternetin bilgiye kolay ulaşma, arkadaşlarla daha sık iletişim kurma, eğitsel materyalleri barındırma, eğlence ve oyun amaçlı kullanımı gibi çeşitli kazanımları varsa da güvenlik tehditleri, siber zorbalık, cinsel içerikler gibi çeşit li çevrimiçi risklerle de karşılaşmaktadırlar (Baştürk Akça, Sayımer ve Ergül, 2015). Özellikle ergen ve çocuk bireylerin çevrimiçi riskler karşısında savunmasız olmalarının sebepleri arasında; deneyimleri, farkındalık düzeyleri, riskleri yönetme durumları ve çevrimiçi risklerden kurtulmak için kullanabilecekleri eleştirel düşünme becerilerinin eksikliği olduğu söylenebilir (OECD, 2011). Bu durumda ise bireylerin fiziksel, duyuşsal ve psikolojik olarak zarar görmeden interneti etkin ve güvenli bir şekilde nasıl kullanılması gerektiği konusu, oldukça önemli hale gelmiştir. OECD (2011) raporunda, bireylerin çevrimiçi risklerden korunmaları için çevrimiçi riskler konusundaki farkındalıklarının artması gerektiği belirtilmiştir. Düzenlenebilecek güvenli

internet kullanımı eğitimleri ve medya ya da internet okuryazarlığının öğretim programlarıyla etkili bir şekilde bütünleştirilmesi ise bireylerin güvenli bir şekilde internet kullanmalarında ve interneti onlar için yararlı hale getirmede faydalı bir strateji olacağı önerilmiştir. Bu raporda özellikle çocukların internet erişimlerinin kısıtlanmasıyla çevrimiçi fırsatlardan yararlanmalarını engellemek yerine, bu ortamların kullanımından doğacak riskler ve fırsatlar konusunda denge sağlayıcı bir politika izlenmesi gerektiğini vurgulamışlardır.

İnternete erişim yaşının da düşmesiyle özellikle internet ortamında karşılaşılabilecek riskler konusunda çocukluk dönemindeki bireyler için güvenli internet kullanımının nasıl sağlanabileceği araştırılmakta (Holloway, Green ve Livingstone, 2013), bu bağlamda özellikle ebeveynlere, çeşitli yasaları yürürlüğe geçirecek kurum ve kuruluşlara ve öğretmenlere olan öneriler artmaktadır. Çeşitli çevrimiçi riskler konusunda yetişkinler düşünüldüğünde ise benzer durumlarla karşılaşılabilmektedir. Özellikle yetişkin olarak tanımlanabilecek ebeveyn, öğretmenler veya genç yetişkinler internet ortamında hangi davranışların kendileri ve çevresindeki bireyler için risk oluşturabileceğini ve daha sonra onlara maddi ya da manevi problemler oluşturabileceklerini genellikle bilmemekte ya da bu bilgiler çok temel düzeyde kalmaktadır. Ergen bireyler ve üniversite öğrencilerinin çevrimiçi riskli davranışlarının incelendiği araştırmada, üniversite öğrencilerinin de çeşitli çevrimiçi riskler aldıklarını belirtmişlerdir. Ayrıca ergenlerin gelişim dönemleri itibarıyla geleceği düşünmeden, bana zarar gelmez düşüncesiyle çeşitli riskli davranışları gerçekleştirirken, üniversite öğrencilerinin bu konuda neden çeşitli riskler aldıklarının daha derinlemesine incelenmesi önerilmiştir (White, Gummerum ve Hanoch, 2017). Alanyazında bu öneriye ilişkin var olan sınırlı çalışmalar incelendiğinde ise çevrimiçi cinsel talepte bulunma davranışı veya kişisel bilgilerin sosyal ağlarda verilmesi gibi çeşitli çevrimiçi riskli davranışlar çerçevesinde hem ergenlerin hem de yetişkinlerin benzer çevrimiçi risk algıları (Baumgartner, Valkenburg ve Peter, 2010) ya da bu davranışların her iki grupta da benzer düzeyde görüldüğü belirtilmiştir (Christofides, Desmarais ve Muise, 2010; Walrave, Vanwesenbeeck ve Heirman, 2012).

Çevrimiçi ortamlarda gençlerin riskli davranışlarının nedenini açıklayan bir başka deyişle bu kararları etkileyen faktörlerin neler olduğunu bütüncül bakışla inceleyen çalışmalar oldukça sınırlıdır. Alanyazındaki çalışmalarda ise bu tespiti destekleyici nitelikte, genç bireylerin çevrimiçi ortamlarda aldıkları riskli kararların nedenlerine inen

ve bu durumlara özgü çözüm getirilecek, farkındalık çalışmaları ve eğitimler gibi çeşitli çalışmaların yapılması gerektiği belirtilmektedir. Yapılan uluslararası çalışmalarda genel olarak bireylerin sıklıkla kullandıkları sosyal ağlara özel gizlilik ve güvenlik ayarlarına göre düzenlenen anketler kullanılarak, hangi çevrimiçi riskli davranışlarda bulundukları ortaya konmaktadır. Çevrimiçi ortamlarda bireylerin kendi güvenliklerini sağlayabilmeleri için sahip olmaları gereken dijital beceriler konusunda da çalışmaların sınırlı sayıda olduğu ya da bu konuda yapılan çalışmaların genel kullanıcı düzeylerine göre ve temel düzeyde oldukları dikkat çekmektedir. Avrupa Ülkeleri bazında gerçekleştirilen çocuk ve internet kapsamındaki projelerde, çocukların karşılaştıkları çevrimiçi risklerin neler olabileceği, ebeveynlerinin bu konudaki bilgi ve becerileri konusunda ve olası çevrimiçi riskler karşısında neler yapılabileceği konusunda tanımlayıcı ve farkındalık oluşturucu geniş çaplı araştırmalar gerçekleştirilmiştir. Çocukların üye oldukları sosyal ağ siteleri, oyunlar gibi sanal profil oluşturdukları ortamlar temelinde yapılan araştırmalarda ise bu ortamlarda çocukların karşılaştıkları riskler ele alınmıştır. Bu ortamlara özgü çocukların çevrimiçi riskli davranışları konusunda cinsiyet, yaş, ebeveynlerin eğitim düzeyleri gibi çeşitli değişkenlerle incelenen birçok çalışmada da bu değişkenler bakımından ilgili profil ortaya konulmuştur. Özellikle çocuklara rehberlik edecek bireyler ele alınarak, karşılaştıkları riskler veya gerçekleştirdikleri riskli davranışların sebeplerini ortaya çıkartacak çalışmaların oldukça sınırlı olduğu görülmüştür. Ergenlikten çıkan ve kendini daha bağımsız hisseden genç bireylerin internet ortamındaki davranışlarının, özellikle çevrimiçi riskli davranışlarda bulunmalarını ve bu konudaki eğilimlerinin ne yönde olduğunu ve çeşitli psiko-sosyal değişkenlerle nasıl açıklandığını gösteren çalışmaların ise oldukça sınırlı olduğu görülmüştür. Bunun yanında konuyla ilgili yapılmış çeşitli ölçeme araçlarının da incelendiği alanyazında, daha çok anketlerin kullanıldığına rastlanmıştır. Bu anlamda çalışmada geçerli ve güvenilir çevrimiçi risk alma eğilimi ve dijital güvenlik öz yeterlik ölçeklerinin geliştirilecek olması alanyazına katkı sağlayacaktır.

1.7. Sınırlıklar

Bu çalışmadaki sınırlılıklar aşağıda maddeler halinde verilmiştir. Bu araştırma

- Çalışma kapsamında geliştirilen Dijital Güvenlik Öz Yeterlik ve Çevrimiçi Risk Alma Eğilimi ölçekleri ile toplanan verilerle,

- 2017-2019 öğretim yılları süresince Eskişehir ili devlet üniversitelerinin dört yıllık fakültelerinde öğrenim gören öğrencilerin katılımıyla,
- Katılımcıların veri toplama araçlarına öz değerlendirme yoluyla verdikleri yanıtlarla,
- Çevrimiçi risk alma eğilimleri kapsamında hem şimdiki ve hem geçmişteki davranışlarını, aynı zaman diliminde ve aynı çevrimiçi riskler çerçevesinde değerlendirmeleriyle,
- Araştırma uygulama verilerinin Anadolu Üniversite'sinde öğrenim gören üniversite öğrencilerinden toplanmasıyla

sınırlıdır.

1.8. Tanımlar

Dijital güvenlik: Dijital tehditlere karşı güvenlik önlemleri almak olarak ifade edilebilir. Ayrıca Internet, e-posta, cep telefonları veya diğer iletişim teknolojilerini kullanırken güvende olmayı tanımlayan bir terimdir (Ribble, Bailey ve Ross, 2004).

Çevrimiçi risk: İnternet teknolojilerinin kullanımından kaynaklanan ve bireylerin fiziksel ya da psikolojik olarak iyi oluşlarını olumsuz yönde etkileyen ihtimallerdir. Uygunsuz içeriklerle karşılaşmak, sosyal medyada hassas kişisel bilgilerin ifşası çevrimiçi risklere örnek verilebilir.

Dijital güvenlik öz yeterliği: Öz yeterlik bir konu hakkında bireylerin bilgi ve becerilerini değerlendirmesidir. İlgili konuda kendi bilgi ve becerilerine olan inancıdır. Dijital güvenlik öz yeterliği ise internet teknolojilerinin güvenli bir şekilde kullanılması için sahip olunan bilgi ve beceriler hakkındaki bireysel değerlendirmelerdir.

Çevrimiçi risk alma eğilimi: Çevrimiçi riskli davranışlarda bulunma sıklığı olarak ifade edilebilir. İlgili davranışın gerçekleştirilme meyilini ifade etmektedir. Bu araştırma kapsamında, şimdiki çevrimiçi risk alma eğilimi ile üniversite öğrencilerinin verilerin toplandığı zaman aralığındaki çevrimiçi risk alma eğilimleri, geçmişteki çevrimiçi risk alma eğilimi ile de lise dönemlerindeki çevrimiçi risk alma eğilimlerinin değerlendirilmesi kastedilmiştir.

1.9. Alanyazın

Bu bölümde çevrimiçi ortamlardaki riskler, çocuk ve yetişkin bireylerin bu ortamlarda gösterdikleri riskli davranışlar, çevrimiçi riskli davranışlarda bulunmayı

etkileyen bazı değişkenlerin odaklanıldığı ve dijital güvenliği sağlama konusundaki çalışmalara yer verilmiştir.

1.9.1. Çevrimiçi risklerle ilgili araştırmalar

Bu bölümde çevrimiçi risklerle ilgili gerçekleştirilen bilimsel çalışmalara yer verilmiştir. Çevrimiçi risklerle ilgili gerçekleştirilen çalışmaların neler olduğu, çevrimiçi rikli davranışları gösteren bireylerin özelliklerinin neler olduğu ve bu davranışlarda nasıl bulunduğu ya da bu davranışlara nasıl maruz kaldığı incelenen değişkenlerle açıklanmaya çalışılmıştır. Ayrıca ilgili çalışmalardaki önemli uygulama ve araştırma önerileri özetlenmiştir.

Pujazon-Zazik, Manasse ve Orrell-Valente (2012), 14-18 yaşı aralığındaki MyLol.net adlı çevrimiçi buluşma web sitesi kullanıcıları olan bireylerin, profillerindeki riskli içerikleri yaş ve cinsiyet değişkenleri bağlamında incelemişlerdir. Profillerde sırasıyla cinsellik, alkol kullanımı, uyuşturucu madde kullanımı, sigara türü ürünler kullanımı ve şiddet konulu riskli içerikler bulunduğu görülmüştür. Araştırmanın bulgularına göre yaşın, herhangi bir riskli içeriği bulundurma davranışının bağımsız belirleyicisi olmadığı görülmüştür. Fakat kadın profillerinin özellikle cinsel konulu riskli içerikleri daha çok barındırdıkları bulunmuştur. Bu durumda çevrimiçi riskler arasında olan siber zorbalık ve cinsel saldırganlık davranışlarının aktörlerine, bu bireylerin hedef kurban olduğu sonucuna varılmıştır. Bu sebeple ergenlik çağındaki bireylerin bu risklerden korunmaları için kitlesel internet politikalarının ve çeşitli güvenli internet kullanımı eğitimlerinin düzenlenmesi gerektiği önerilmiştir.

Soldatova ve Zotova (2013) çalışmasında Rus okul öğrencilerinin siber zorbalık ve cinsel içeriklerle ilgili olan çevrimiçi riskler hakkındaki algılarını ve bu zorluklarla başa çıkma stratejilerini belirlemeyi amaçlamışlardır. Rus çocuklarının Avrupa ülkelerindeki çocuklara kıyasla daha fazla siber zorbalık ve cinsel içerikler türündeki çevrimiçi risklerle karşılaştıkları belirlenmiştir. Cinsel içerikli risklerle karşılaştıkları zaman erkeklerin, kadınlara göre daha çok aktif başa çıkma stratejilerini kullandıkları bulunmuştur. Ayrıca bu tür çevrimiçi risk karşısında en çok kullanılan pasif stratejiler ise internet kullanmaya bir süreliğine ara vermek olduğu görülmüştür. Genel olarak siber zorbalık durumunda cinsel içeriklere oranla aktif stratejilerin iki kat daha fazla seçtikleri belirlenmiştir. Her iki risk türünde de sosyal destek almanın ikincil olarak tercih edildiği görülmüştür. Bu çalışmada çocuklar ve yetişkinler arasında önemli bir dijital uçurum olduğunu ve bu

durumun çeşitli çevrimiçi riskler karşısında destek almalarını azalttığı sonucuna ulaşılmıştır.

Yenilmez ve Seferoğlu (2013), çalışmalarında sanal zorbalık ve öğretmenlerin sanal zorbalık hakkındaki farkındalıklarını incelemişlerdir. Türkiye'nin çeşitli illerinde görev yapan 583 öğretmen adayının katıldığı bu çalışmada öğretmenlerin sanal zorbalık konusundaki genel farkındalıklarının yüksek olduğu bulunmuştur. Öğretmenlerin bulundukları okulların sosyo-ekonomik düzeyleri ve internet kullanım sıklıkları sanal zorbalık hakkındaki görüşleri üzerinde etkili olduğu, cinsiyet ve internet kullanım süresinin doğrudan bir etkisinin olmadığı bulunmuştur. Sanal zorbalık riskinin betimsel olarak incelendiği bu çalışmada, öğretmenlerin çevrimiçi riskler hakkında bilinçli olmaları ve bu konuda örnek olabilmeleri için çevrimiçi riskler hakkında eğitim almaları gerektiği önerilmiştir. İnternetin sadece riskleri barındıran bir ortam olmadığı aynı zamanda çocukların çevrimiçi fırsatlardan yararlanmalarını sağlayan bir ortam olduğu vurgulanmıştır. Çocukların olası çevrimiçi riskler konusunda bilinçlenmeleri ve bu risklerle başa çıkabilmelerini sağlayacak uygulamalar ve ortamların oluşturulması gerektiğini belirtmişlerdir.

Kaşıkçı, Çağıltay, Karakuş, Kurşun ve Ogan (2014) EU Kids Online II araştırmasının Türkiye'de gerçekleştirilen bölümünü üstlenmişlerdir. Bu çalışmada çocukların karşılaştıkları çevrimiçi riskleri incelemişlerdir. 1018 çocuğun ve ebeveynlerinin katıldığı bu araştırma ilgili konuda yapılan ulusal çaptaki en kapsamlı çalışmadır. Bu çalışmanın sonucunda Türkiye'deki çocukların çevrimiçi risklerle karşılaşma oranlarının %25 olduğu ve bu oranın Avrupa ile kıyaslandığında %33 ortalamanın altında olduğu görülmektedir. Bu oranlara bakıldığında çocukların çevrimiçi risklere maruz kaldığı, ebeveynlerinin ise çocuklarını karşılaşabilecekleri çevrimiçi risklerden koruyabilecek düzeyde bilgilerinin olmadığı görülmüştür.

White, Gummerum ve Hanoch (2015), gençlerin kişisel bilgi paylaşımı ve çevrimiçi ortamlarda tanımadığı kişilerle arkadaşlık kurma gibi riskli çevrimiçi aktivitelerle karşılaştıklarını ve bu aktivitelere katıldıkları belirtmiştir. Gençlerin çevrimiçi risk almalarının altında psikolojik mekanizmaların yattığını vurgulamışlardır. Bu doğrultuda da Bulanık İz Teorisi çerçevesini kullanarak ergenlerin ve genç yetişkinlerin çevrimiçi risk almada gelişimsel farklılıklarını açıklamayı ve davranış değerlendirme yollarına (gist based ve verbtaim based) dayalı faktörlerin çevrimiçi risk alma davranışını açıklayıp açıklamadığını araştırmayı amaçlamışlardır. Çalışmaya 13-17

yaş aralığındaki 122 ergen birey ve 18-24 yaş aralığındaki 172 birey katılmıştır. Geçmiş çevrimiçi risk alma davranışları, gelecekteki çevrimiçi riskli davranışlara katılım niyetleri ve davranış değerlendirme yolları belirlenmiştir. Ergen bireylerin genç yetişkinlere göre çevrimiçi risk alama konusundaki niyetlerinin anlamlı düzeyde yüksek çıkmıştır. Ergenlerde geçmiş riskli çevrimiçi davranışları ile gelecekte riskli çevrimiçi davranış niyeti arasında pozitif yönde bir ilişki çıkmıştır. Bu durum genç yetişkinlerde negatif yöndedir. Risk hakkında gist based düşünme yolları ile çevrimiçi riskli davranış niyetleri arasında her iki grupta nagatif bir ilişki çıkarken, özellikle ergenlerde verbtaim based düşünme yolları ile çevrimiçi risk alma niyetleri arasında pozitif yönde bir ilişki bulunmuştur.

Byrne, Dvorak, Peters, Ray, Howe ve Sanchez (2016) çalışmasında, 19-68 yaş aralığındaki yetişkin bireylerin sıklıkla gerçekleştirdikleri internet kullanımındaki davranışları belirlemişlerdir. Daha sonra bu davranışları hangi amaçla gerçekleştirdikleri ve bu davranışlara ilişkin algıladıkları riskler belirlenmiştir. Ayrıca listelenen davranışları hangi sıklıkta gösterdikleri ve bu davranışları gerçekleştirirken ne kadar miktarda bilgi paylaşmayı istedikleri de ele alınmıştır. Katılımcıların bazı internet kullanımı eylemlerini riskli bulduklarını belirtmişlerdir. Bu davranışları göstermelerinin nedeni olarak da ilgili kullanım davranışından sağladıkları yarar veya edindikleri kazanım olarak açıklamışlardır. Katılımcıların birçok internet eyleminde fazla kişisel bilgi verme eğiliminde olmadıkları bulunmuştur. Fakat çevrimiçi bankacılık, çevrimiçi alış-veriş gibi eylemlerin de daha fazla kişisel bilgi gerektirdiğini belirtilmiştir. Bunu da algılanan riskle ilişkili olduğu belirtilen, internete duyulan güvenle açıklamaya çalışmışlardır.

White Gummerum, Wood ve Hanoch (2017) un 18-79 yaş aralığındaki 326 yetişkin katılımcıyla gerçekleştirdikleri araştırmada, yetişkinlerin çevrimiçi riskli davranışları ve bu davranışlara olan niyetleri incelenmiştir. Alanyazında yetişkinlerin internet kullanımı ve bu süreçte karşılaştıkları çevrimiçi riskler ve çevrimiçi riskli davranışlarının neler olduğuna ilişkin çok az sayıda çalışmanın yer aldığını vurgulamışlardır. Yaş değişkeninin geçmiş risk alma davranışları ile negatif bir ilişki gösterdiği, internet kullanım süresinin ise gelecekteki risk alma niyetleri ile pozitif ilişki gösterdiği bulunmuştur. Yaş değişkeni gözetilmeksizin genel olarak her yaştaki bireyler kişisel bilgilerin paylaşımı ile ilgili çeşitli riskler almaktadırlar. Çalışmaya katılan bireylerin üçte birinden fazlası sosyal ağlarda yabancı kişilerle arkadaş olmakta, gerçek hayatta tanımadıkları bu kişilerle bir ilişki geliştirmektedirler.

Gamez-Guadix, De Santisteban ve Alcazar (2017) çalışmasında, yetişkin bireylerin daha genç bireyler ile çevrimiçi ortamlarda cinsel sosyalleşme davranışlarını incelemek için geçerli ve güvenilir bir ölçme aracı geliştirmeyi amaçlamışlardır. Bu çalışma bağlamında genellikle yaşlı yetişkinlerin çevrimiçi riskler konusunda genç yetişkinlerden daha az bilgiye sahip olduklarını vurgulamışlardır. Ayrıca çevrimiçi ortamlar aracılığıyla oluşan cinsel sosyalleşme veya cinsel içerikli iletişim ve etkileşimlerin genellikle yetişkinler tarafından gerçekleştirildiğini belirtmişlerdir. "Bir yetişkin benden kendimle ilgili seksi bir fotoğraf veya video istedi" gibi riskli davranışlara genellikle yetişkin bireylerin sebebiyet verdiğini vurgulamışlardır.

Çevrimiçi riskler hakkında ilgili literatür irdelendiğinde, çevrimiçi teknolojileri veya çeşitli çevrimiçi platformları çocukların kullanım sıklıklarının artması ve çocukların bu ortamlardaki savunmasızlıkları sebebiyle çevrimiçi riskler konusu önem kazanmıştır. İlgili literatürde bireylerin internet teknolojilerini kullanım amaçları incelenmiş ve genellikle bu ortamlarda hangi davranışları gerçekleştirdikleri belirlenmiştir. Bunun yanında gerçekleştirilen çevrimiçi davranışların kişisel bilgilerin ifşa edilmesi, uygunsuz içeriklerin oluşturulması ve paylaşılması gibi hangilerinin riskli olduğu ve bu riskli çevrimiçi davranışların gerçekleştirilme nedenlerinin, yaş, cinsiyet gibi demografik değişkenlerin yanında, bireylerin karar verme stilleri, risklerden kaçınma stratejileri, algılanan fayda, risk algısı, güven gibi değişkenlerle incelendiği görülmektedir. Genellikle çevrimiçi riskli davranışlar arasında kişisel bilgilerin ifşası, uygun olmayan içeriklerle karşılaşılması ya da bu tür içeriklerin oluşturulup paylaşılması, uygunsuz çevrimiçi sosyalleşme ve cinsel sosyalleşme ve siber zorba olma ya da siber zorbalara maruz kalma gibi davranışlar yer almaktadır. Çocukluk dönemindeki bireylerin ve yetişkinlik dönemlindeki bireylerin çevrimiçi riskli davranışlarda bulunma sebeplerinin içinde bulundukları gelişim döneminden kaynaklanan davranışı değerlendirme yetilerinin gelişmişlik düzeylerinden kaynaklanmasının yanında, özellikle gerçekleştirilen herhangi bir çevrimiçi davranışın risk barındırıp barındırmadığı konusunda farkındalık düzeylerinin oldukça düşük olması olduğu söylenebilir.

1.9.2. Dijital güvenlik ile ilgili araştırmalar

Bu bölümde dijital güvenliği sağlama konusunda gerçekleştirilen bilimsel çalışmalara yer verilmiştir. Dijital güvenlikle ilgili gerçekleştirilen çalışmaların neler olduğu, dijital güvenliği sağlamak için hangi bilgi ve becerilere sahip olunması gerektiği,

dijital güvenliği sağlamada hangi değişkenlerin önemli olduğu açıklanmaya çalışılmıştır. Ayrıca ilgili çalışmalardaki önemli uygulama ve araştırma önerileri özetlenmiştir.

Demirel, Yörük ve Özkan (2012), çalışmalarında ebeveynlerin Bilgi Teknolojileri ve İletişim Kurumu tarafından yürütülen "Güvenli İnternet Hizmeti" projesi hakkında görüşlerini incelenmiştir. 247 öğrencinin ebeveynlerine anket uygulanarak yapılan bu çalışmada öğrencilerin %68'inin evinde internet bağlantısının bulunduğunu, ebeveynlerin %75,3'ünün internetin çocukları için güvensiz bir ortam olduğunu düşündükleri bulunmuştur. Ayrıca "Güvenli İnternet Hizmeti" projesinden ebeveynlerin %68,4'ünün haberdar olduğu fakat %36,9'unun internet filtresi kullandığı belirtilmiştir. İnternet filtresini kullanan ailelerin %87,1'i "Aile Profilini" kullanırken %12,9'unun ise "Çocuk Profilini" kullandığı bulunmuştur. Çalışmada internetin riskleri ile hem yetişkinlerin hem de çocukların, internet kullanım oranları arttıkça daha fazla karşılaşılacağı, bu durumda da çocuk ve genç bireylerin nasıl korunması gerektiği konusunda çalışmalar yapılması gerektiği önerilmektedir.

Tokel, Başer ve İşler (2013), Ankara'nın farklı bölgelerinde yaşayan ilköğretim öğrencileri ebeveynlerine "Bilgi Toplumunda Aile" seminerleri düzenlenerek, ebeveynlerin bilgisayar, internet ve sosyal paylaşım siteleri kullanımına yönelik algıları ve bilgi seviyeleri incelenmiştir. Ebeveynlerin bilgisayar ve internet kullanımı konusunda çocuklarına yardım etmeleri için yeterli düzeyde farkındalıkları ve bilgileri olmadığı, sosyal paylaşım sitelerine çocuklarını takip etmek amacıyla üye olsalar da bu siteleri kullanım süreleri çocuklarından oldukça az olduğu görülmüştür. Bu durumda da çocuklarının sosyal paylaşım sitelerinde takip etme düzeylerinin yetersiz olduğu belirtilmiştir. Ayrıca çocukların bu teknolojileri kullanmaları konusunda yeterli bilgiye sahip olmamaları, teknolojileri kullanmalarını yasaklamakta ya da kısıtlamalara başvurduklarını gösterdiğini vurgulamışlardır. Ebeveynler çocuklarının sosyal paylaşım sitelerini kullanma konusunda ise eğitim amaçlı ve sosyal ilişkilerini geliştirme konusunda faydalı olduğunu düşünseler bile vakit kaybına, olumsuz arkadaşlık ilişkileri geliştirmelerine sebep oldukları, saygısız davranışlar ve güvenlik tehditleri oluşturdukları için çocuklarının bu siteleri kullanmalarını onaylamadıkları ortaya çıkmıştır. Çocukların bilgisayar, internet ve sosyal paylaşım siteleri kullanımını kısıtlamaktan ziyade sınırlayıp güvenlik önlemlerini alarak bu sürece ebeveynlerin aktif katılımı sağlanabileceği önerilmiştir. Buna ek olarak bu konuda yapılacak yeni araştırmalarda ebeveynlerin eğitim düzeyleri ve ebeveynlik tipleri gibi faktörlerin incelenmesi önerilmiştir.

Baştürk Akça, Sayımer ve Ergül (2015), çalışmasında ergenlerin sosyal medya kullanımlarını ve siber zorbalık deneyimleri araştırmışlardır. Ankara'da ortaokul 7. ve 8. sınıf düzeyindeki 200 öğrenci ile betimsel bir araştırma yürütülmüştür. Öğrencilerin çoğunun evinde internete erişim olduğu ve her gün en az bir kere sosyal ağ hesaplarını ziyaret ettikleri bulunmuştur. Öğrencilerin %24'ünün siber zorbalık/mağduriyet deneyimlerinin olduğu belirlenmiştir. Cinsiyete göre siber zorbalık deneyimleri incelendiğinde erkeklerin kızlara oranla daha fazla siber saldırgan oldukları görülmüştür. Bu durumda ergenlerin internet ortamında karşılaşabilecekleri risklerle mücadele edebilmek için bilinç ve farkındalık arttırıcı uygulamaların yapılması gerektiği önerilmiştir. Özellikle internet kullanımını yasaklayıcı önlemler alınmaması gerektiği vurgulanmıştır.

İnternet kullanımının oranının artması ve bu oranda karşılaşılan çevrimiçi risklerin de artmasıyla bireylerin siber ortamdaki güvenlikleri konusu oldukça önemli hale gelmiştir. Bu nedenle Erol, Şahin, Yılmaz ve Haseski (2015) çalışmasında internet kullanıcılarının siber güvenlik ile ilgili davranışlarını belirlemeye yönelik bir ölçek geliştirmişlerdir. Ölçme aracının geliştirilmesinde Facebook sosyal paylaşım ağı kullanıcıları olan 810 kişiye ulaşılmıştır. Daha sonra yine Facebook kullanıcıları olan ve ölçme aracını geliştirmede kullanılmayan 292 katılımcı verileri kullanılarak ölçek doğrulanmıştır. Oluşturulan "Kişisel Siber Güvenliği Sağlama Ölçeği"; kişisel gizliliği koruma, güvenilmeyenden kaçınma, önlem alma, ödeme bilgilerini koruma ve iz bırakmama olmak üzere 5 faktör ve toplamda 25 maddeden oluşmaktadır. Oluşturulan ölçeğin güvenirlik katsayısı 0.735 iken, toplam varyansın %48.026'sını açıkladığı bulunmuştur. Bu ölçeğin çeşitli bağımsız değişkenlerle karşılaştırılarak incelenmesi ve ortaokul, lise, üniversite öğrencileri ve öğretmenler gibi farklı örneklem gruplarında uygulanarak test edilmesi önerilmiştir.

Ceyhan, Demiryürek ve Kandemir (2015), çalışmasında sosyal ağlar ve bu ağların güvenlik problemleri incelenmiş ve karşılaşılan problemlere karşı bireysel ve kurumsal olarak alınabilecek güvenlik önlemlerinin sunulması amaçlanmıştır. En sık kullanılan sosyal ağlar arasında Facebook, Twitter, YouTube, Linked-in, Google+, Instagram, Flicker, Myspace, Blogger ve Skype yer almaktadır. Bu çalışma sonucunda ulusal olarak sosyal ağlarda bilgi gizliliği ve güvenliğini koruma konusunda karşılaşılan çeşitli risklere değinilmiştir. Bu riskler arasında kimlik hırsızlığı ve e-dolandırıcılık yer almaktadır. E-dolandırıcılık türleri olarak da iyi bilenen şirketlerin adlarını kullanma, piyango

dolandırıcılıkları, sahte güvenlik yazılımı dolandırıcılıkları, profil klonlama, üçüncü şahıs uygulama tehlikeleri, sahte ürün satışı, kötü bağlantı istekleri, istenmeyen e-postalar ve kötü niyetli yazılımlar bulunmaktadır. Bu tehlikeler karşısında çocukların ve gençlerin korunması için çeşitli hukuki boşlukların doldurulması gerektiği, hükümet, eğitim kurumları ve bireylerin birlikte çalışmaları gerektiği önerilmiştir.

Jeske ve Van Schaik (2016), internet tutumları ve güvenlik davranışlarının tahmin edicilerinin dijital tehditler olduğunu öne sürerek 323 üniversite öğrencisiyle bir araştırma gerçekleştirmişlerdir. Katılımcılara 16 farklı internet tehdidinin ne anlama geldiği ve bu tehditlere ne kadar aşina oldukları sorulmuştur. Bu doğrultuda yapılan kümelemede üç grup ortaya çıkmıştır. Bu gruplar genellikle tehditlerin tümünün ne olduğunu bilen, iyi bilinen tehditlere aşina olanlar ve yeni tehditlere aşina olanlar şeklindedir. Tehditlerin tümünü bilen gruptaki katılımcılar diğer gruptakilere göre antivirüs, güvenlik duvarı, anti-casus yazılımı kullanma ve yazılım güncellemeleri gibi bilgisayar güvenliği davranışları sergiledikleri, internette harcanan sürenin ve internet deneyimlerinin uzunluğunun internet tehditlerine aşinalığın önemli yordayıcıları olduğu ve bilgisayar güvenliği kullanımının doğrudan olmayan önemli bir tahmin edicisi olmuştur. Ayrıca çalışmada internet tehditlerine olan aşinalığın, internet kullanımı ve güvenlik davranışları arasında arabulucu bir değişken olduğu ortaya çıkmıştır. Sonuç olarak internet tehditlerine fazla aşinalık tam olarak daha iyi bilgisayar güvenliğinin sağlanmasıyla el ele gitmediği ortaya çıkmıştır. İnternet tehditlerine ve farklı çevrimiçi davranışlara aşinalık, bu tehditlerin yeniliğine ya da iyi bilinen tehditler olmalarına bağlı olabileceği ortaya koyulmuştur.

Schaik, Jeske, Onibokun, Coventry, Jansen ve Kusev (2017) çalışmasında, 436 üniversite öğrencisi ile 16 dijital güvenlik zararı kapsamında çevrimiçi risk alma algılarını ve bu tehditlerden kaçınma davranışlarını belirlemeye çalışmışlardır. Katılımcılar en riskli dijital tehlikenin kimlik hırsızlığı, en az riskli olan ise çerezler ve e-posta edinmek olarak algıladıklarını belirtmişlerdir. Katılımcıların çoğunluğunun antivirüs yazılımı kullanma, işletim sistemi güncellemeleri ve güvenlik yazılımı kurma gibi dijital güvenlik becerilerinin yüksek olduğu bulunmuştur. Genellikle bireylerin dijital güvenlik zararları kapsamında daha önce yaşamış oldukları olumsuz deneyimlerin, ilgili davranış konusundaki risk algılarını arttırdığını ifade etmişlerdir. Dolayısıyla bu çalışmada katılımcıların internet deneyimlerinin algıladıkları riskin önemli bir öngörücüsü olduğu vurgulanmıştır.

Parsons, Calic, Pattinson, Butavicius, McCormac ve Zwaans (2017) çalışmasında, çevrimiçi ortamlarda bilgi güvenliği davranışları konusunda 112 üniversite öğrencisinin katıldığı bir sormaca geliştirmişlerdir. Bu sormacaya katılan öğrenciler aynı zamanda siber bir atak ortamı düzenlenen deneye de katılmışlardır. Sormacada şifre yönetimi, e-posta kullanımı, internet kullanımı, sosyal medya kullanımı, mobil araçların kullanımı, bilgiyle başa çıkabilme ve rapor bildirme gibi odaklanılan alanlar mevcuttur. Örneğin aynı şifreyi her hesapta kullanmak ya da şifreyi paylaşmak gibi şifre yönetiminde ele alınan alt boyutlar bulunmaktadır. Çalışmanın sonuçları ele alındığında sormacada yüksek skorlara sahip katılımcıların siber saldırı deneyinde de daha başarılı performans gösterdikleri ortaya çıkmıştır. Bu nedenle sormacanın bilgi güvenliği davranışlarını tahmin ettiği ortaya çıkmıştır. Daha sonra bu sormaca 531 yetişkine uygulanmış ve bu sormaca için ölçek geliştirmede kullanılan geçerlik güvenirlik çalışmaları yürütülmüştür. Bu çalışmanın sonucunda da birinci çalışmadan elde edilen yapıya ulaşılmıştır. Dolayısıyla siber güvenlik konusunda bilgi güvenliği davranışları sormacasının yapı geçerliği sağlanmıştır.

Gratian, Bandi, Cukier, Dykstra ve Ginther (2018) çalışmasında, 369 üniversite öğrencisi, öğretim üyesi ve idari personelden oluşan yetişkin bireylerin kişilik özellikleri ile siber güvenlik davranışları niyetleri arasındaki ilişkileri ortaya koymuştur. Katılımcıların risk alma tercihleri, karar verme stilleri, demografik özellikleri ve kişilik özelliklerinin araç güvenliği, şifre üretimi, önleyici farkındalıkları ve güncelleme güvenlik davranışları niyetleri üzerinde kapsamlı bir araştırma yürütülmüştür. Katılımcıların risk alma tercihlerinin kullandıkları dijital araçların güvenliği ile ilgili niyetleri ile ilişkili bulunmamıştır. Katılımcıların demografik özelliklerinin şifre belirleme güvenlik davranışı niyeti üzerinde önemli bir öngörücü olduğu ortaya çıkmıştır. Demografik faktörler açısından özellikle cinsiyet önceliyi farkındalık güvenlik davranışı niyeti üzerinde önemli bir öngörücü olmuştur. Çünkü kadın katılımcılar erkeklerden daha az önleyici farkındalıkları olduğunu belirtmişlerdir. Güncelleme güvenlik davranışı niyetinde de cinsiyet konusunda benzer bulguya ulaşılmıştır. Hatta bu doğrultuda kadınların daha zayıf güvenlik davranışı niyetleri olduğu sonucuna varılmıştır. Özellikle finansal risk alma, rasyonel karar verme ve cinsiyet gibi karakteristik özellikler iyi güvenlik davranışı niyetlerinin önemli birer yordayıcısı olduğu ortaya çıkmıştır.

Dijital güvenlik ile ilgili incelenen alanyazında, çevrimiçi platformlar veya hizmetlerin ve internet erişimin sağlandığı teknolojik araçların bilinçli ve güvenli bir

şekilde kullanımını kapsayan çeşitli bilgi ve becerilerin neler olduğu, güvenli internet teknolojilerinin kullanımı için planlanmış deneyim kazandırıcı uygulamalar ve bu konudaki farkındalık, tutum veya yeterlik ölçme araçları konularında çalışmalar yer almaktadır. İlgili literatürde dijital güvenliği sağlamada yaş, cinsiyet, internet kullanım deneyimi ya da sıklığı gibi demografik değişkenlerin yanında, arabulucukuk türleri, risk alma, güven ve rasyonel karar verme değişkenleriyle incelenmiştir. Genellikle uygulama yapılan deneysel araştırmalarda ise örneğin Facebook sosyal ağının gizlilik ve güvenlik ayarlarının yapılandırılması gibi kullanılan teknolojiye özgü güvenli kullanım becerilerinin kazandırılması amaçlanmıştır. Bunun yanında çeşitli çalışmalarda ise, virüs programı kullanma, güncelleme yapma, şifreleme gibi hem teknik, kişisel bilgilerini ifşa etmeme, bilinmeyen sitelerden alışveriş yapmama gibi hem de davranışsal olarak önlem alma becerilerinin değerlendirilmesi ve kazandırılması amaçlanmıştır. Bu çalışmalar yapılırken de genellikle bilgi, beceri, tutum ve davranışlar, kullanılan teknolojilere özgü güvenlik boyutları doğrultusunda hazırlanan anketler ve sormacalarla ölçülmüştür. Yapılan çalışmalarda tüm internet teknolojileri kullanıcılarının ilgili teknolojilerin güvenli bir şekilde kullanabilmeleri için farkındalık ve beceri kazandıracak eğitim uygulamalarının yapılması gerektiği önerilmiştir.

2. YÖNTEM

Bu bölümde, gerçekleştirilen araştırmanın modeli, evren ve katılımcılar, veri toplama araçlarının geliştirilmesi, veri toplama araçları ve araştırma verilerinin çözümlenmesinde kullanılan istatistiksel teknikler açıklanmıştır.

2.1. Araştırma Modeli

Bu çalışma, tarama türü araştırma olarak desenlenmiştir. Nicel bir araştırma yaklaşımı temel alan bu tür belirli bir konu hakkında evren veya örneklemde tutum, fikir, davranış ya da ilgili örneklemin karakteristik özelliklerini ortaya koymayı hedefler. İncelenen konu hakkında var olan durumu olduğu gibi betimlenmeye imkân veren bir modeldir. Aynı zamanda bu modeller, olayların içinde bulunduğu koşulları ve bu koşullar arasındaki ilişkilerin belirlenmesi için kullanılırlar (Creswell, 2012). Tarama modellerinin ise tekil tarama, ilişkisel ve nedensel karşılaştırma türleri bulunmaktadır (Karasar, 2009). Bu çalışmada da araştırmaya katılan üniversite öğrencilerinin demografik özellikleri, dijital güvenlik öz yeterlikleri ve çevrimiçi risk alma eğilimlerini belirlemek amacıyla tekil tarama, kuramsal teoriler yoluyla belirlenen değişkenler arası hipotezleri test etmek için ilişkisel tarama türü tarama modelleri kullanılmıştır.

2.2. Çalışma Grubu

Araştırmanın evrenini 2016-2017, yılında Tablo 2.1'de yer alan Eskişehir ili devlet üniversitelerinde 4 yıllık fakültelerde örgün öğrenim görmekte olan öğrenciler (n=45520) oluşturmaktadır. Bu evrenin tamamına ulaşmak ekonomi, zaman ve uygulama konusunda güçlük oluşturacağından evreni temsil eden örneklem belirleme yoluna gidilmiştir. Bu aşamada ise Tablo 2.1'de yer alan Anadolu Üniversitesi ve Eskişehir Osmangazi Üniversitesi'nde bulunan fakülteler kullanılmıştır. Eskişehir ili devlet üniversitelerini temsil eden bu fakülteler sebebiyle tabakalı örnekleme, bu fakültelerde bulunan bölümlerden seçilen bölümlere ulaşarak amaçlı örnekleme yöntemi ile araştırmanın katılımcıları belirlenmesi planlanmıştır.

Tablo 2.1. *Eskişehir ili devlet üniversitelerinin dört yıllık fakülteleri ve öğrenci sayıları*

Üniversiteler	Fakülteler	Öğrenci Sayıları
Anadolu Üniversitesi	İktisadi ve İdari Bilimler Fakültesi	4199*
	Eğitim Fakültesi	3940*

Tablo 2.1. (Devam) *Eskişehir ili devlet üniversitelerinin dört yıllık fakülteleri ve öğrenci sayıları*

Üniversiteler	Fakülteler	Öğrenci Sayıları
Anadolu Üniversitesi	İletişim Bilimleri Fakültesi	1634
	Güzel Sanatlar Fakültesi	760
	Eczacılık Fakültesi	761
	Edebiyat Fakültesi	2052*
	Hukuk Fakültesi	1822
	Fen Fakültesi	1564
	Havacılık ve Uzay Bilimleri Fakültesi	933
	Mimarlık ve Tasarım Fakültesi	1393
	Mühendislik Fakültesi	3005*
	Sağlık Bilimleri Fakültesi	345
	Spor Bilimleri Fakültesi	730
	Turizm Fakültesi	620
Ara Toplam		23758
Eskişehir Osmangazi Üniversitesi	Tıp Fakültesi	1356
	Diş Hekimliği	226
	Eğitim Fakültesi	2464*
	Fen Edebiyat Fakültesi	4187*
	Ziraat Fakültesi	710
	Mühendislik Mimarlık Fakültesi	7115*
	Sanat ve Tasarım Fakültesi	117
	İktisadi ve İdari Bilimler Fakültesi	3637*
	İlahiyat Fakültesi	1190
	Turizm Fakültesi	760
Ara Toplam		21762
Genel Toplam		45520

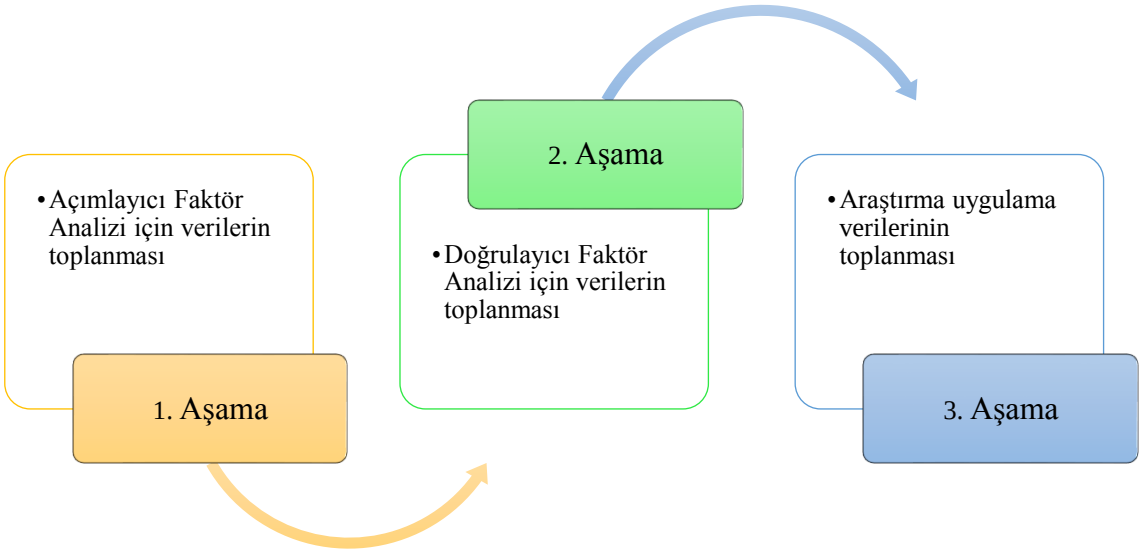
*Öğrenci sayısı 2000 ve üstü üzerinde olan fakülteler

Araştırma verilerinin toplanacağı katılımcı sayıları evreni temsil edebilecek örneklem formülleri ve %65 geri dönüş oranı kullanılarak hesaplanmıştır. Evren ve örneklem bilgileri ve yapılan hesaplamalar aşağıda görülmektedir.

- Örneklem hesaplama formülü; $n_0= (t)^2 * (p)(q) /(d)^2$

Formülde; t= seçilen güven düzeyi (%99), (p)(q) = maksimum örneklem büyüklüğü için varyans tahminini (0,5) (0,5), d= kabul edilebilir hata payını (%3) temsil etmektedir. Bu formülü temel alıp oluşturulan ve http://www.surveysystem.com/sscalc.htm adresinde örneklem sayısı belirleme motoru işe koşulduğunda, 45520 kişilik evreni temsil edebilecek örneklem sayısının en az 1777 kişiden oluşması gerektiği ortaya çıkmıştır. Öz değerlendirmeler yoluyla toplanan verilerde, katılımın geri dönüş oranının da örneklem sayısını belirlemede hesaba katılmasını gerektirmektedir. Geri dönüş olarak %65 varsayımı temel alındığında örneklem sayısının 2933 kişiden oluşması planlanmıştır. Araştırmanın veri toplama bölümü üç aşamada tamamlanmıştır. Bu aşamalar Şekil 2.1'de görülmekte olan Açımlayıcı Faktör Analizi, Doğrulayıcı Faktör Analizi ve Araştırma

Uygulama Verileri için verilerin toplanması aşamalarını kapsamaktadır. Birinci ve ikinci aşamada geliştirilmesi planlanan ölçekler için yeterli katılımcıya ulaşılması esas alınmıştır. Ayrıca ölçeklerin geliştirilmesinin her aşamasında aynı katılımcılardan veri toplanmaması için ölçeklerin açımlayıcı faktör analizi aşamasında Anadolu Üniversitesi, doğrulayıcı faktör analizi aşaması için Eskişehir Osmangazi Üniversitesi öğrencilerinden veri toplanmıştır. Araştırmanın uygulama verileri ise Anadolu Üniversitesi bünyesinde toplanmıştır.



Şekil 2.1. *Araştırma verileri toplanması süreci*

Birinci veri toplama aşaması katılımcıları 490 üniversite öğrencisinden oluşmaktadır. Eskişehir ili devlet üniversitelerinin 4 yıllık fakülteleri ve öğrenci sayıları verilen Tablo 2.1'deki Anadolu Üniversite'sinde öğrenim görmekte olan ve sayıları 2000 üzerinde olan dört yıllık fakültelerden bu veriler elde edilmiştir. Sayısı 2000'in üzerinde öğrenim gören öğrencisi bulunan fakültelerden veri toplanmasının nedeni ise araştırma verileri toplanırken aynı katılımcılardan veri toplamanın önüne geçilmesidir. Araştırmanın birinci aşaması katılımcıları ile ilgili ayrıntılı bilgi 2.4.4. Aday DGÖY ölçeğinin AFA aşaması katılımcıları başlığında sunulmuştur. İkinci veri toplama aşaması katılımcıları 939 üniversite öğrencisinden oluşmaktadır. Eskişehir ili devlet üniversitelerinin 4 yıllık fakülteleri ve öğrenci sayıları verilen Tablo 2.1'deki Eskişehir Osmangazi Üniversite'sinde öğrenim görmekte olan ve sayıları 2000 üzerinde olan dört yıllık fakültelerden bu veriler elde edilmiştir. Sayısı 2000 in üzerinde öğrenim gören öğrencisi bulunan fakültelerden veri toplanmasının nedeni ise araştırma verileri

toplanırken aynı katılımcılardan veri toplamanın önüne geçilmesidir. Araştırmanın ikinci aşaması katılımcıları ile ilgili ayrıntılı bilgi 2.4.6. Aday DGÖY ölçeğinin DFA aşaması katılımcıları ve 2.5.6. Aday ÇRAE ölçeği DFA aşaması katılımcıları bölümlerinde sunulmuştur. Üçüncü veri toplama aşaması katılımcıları 1601 üniversite öğrencisinden oluşmaktadır. Tablo 2.2'de yer alan Anadolu Üniversite'sindeki dört yıllık öğrenim sağlayan fakültelerden araştırma uygulama verileri toplanmıştır.

Tablo 2.2. *Araştırma uygulama verilerinin toplandığı fakülteler*

Veri Toplanan Fakülteler	Veri Toplanamayan Fakülteler
Eczacılık Fakültesi	Güzel Sanatlar Fakültesi
Edebiyat Fakültesi	Havacılık ve Uzay Sanatları Fakültesi
Eğitim Fakültesi	Sağlık Bilimleri Fakültesi
Fen Fakültesi	Spor Bilimleri Fakültesi
Hukuk Fakültesi	
İktisadi ve İdari Bilimler Fakültesi	
İletişim Bilimleri Fakültesi	
Mühendislik ve Mimarlık Fakültesi	
Turizm Fakültesi	

Verilerin toplanması aşamasında hem etik kurul hem de araştırma uygulama izni olduğu halde Tablo 2.2'de yer alan bazı fakültelerde idari ve akademik personelin veri toplamaya onay vermemesi ve öğretim faaliyetlerinin birebir ve uygulamalı olması sebebiyle veri toplama işlemi gerçekleştirilememiştir. Anadolu Üniversitesi'nden veri toplanabilen 20990 öğrenciyi temsil edebilmek için yukarıdaki örneklem hesaplamaları işe koşulduğunda 1699 sayıda katılımcıya ulaşılması gerekmiştir. Araştırma uygulama verileri kapsamında 1729 sayıda katılımcıya ulaşılmıştır. Ölçme araçlarının yarısından fazlasına katılım göstermeyen ve uç değer niteliğindeki veriler veri setinden çıkartıldığında verileri analize tabi tutulan katılımcı sayısı 1601'e düşmüştür. İlgili katılımcı bilgileri ve özellikleri Tablo 2. 3 ve Tablo 2. 4'te ayrıntılı olarak belirtilmiştir. Dolayısıyla ulaşılan örneklemin evreni yüksek oranda temsil ettiği söylenebilir.

Araştırma uygulama aşamasında analize tabi tutulan 1601 katılımcı mevcuttur. Bu katılımcıların yaklaşık 974 (%61)'ü kadın, 622 (%39)'si erkek üniversite öğrencilerinden oluşmaktadır. Katılımcılardan 5 (%0,3)'i ise cinsiyet bilgisini belirtmemiştir. Tablo 2. 3 incelendiğinde araştırma katılımcılarının yaş aralıkları 18-39 aralığında değişmektedir. Anadolu Üniversitesi'nin 10 farklı fakültesinde öğrenim gören bu katılımcıların 974 (%61)'ü kadın, 622 (%39)'i erkektir. Araştırmanın uygulama katılımcılarına ilişkin ayrıntılı bilgi ve özellikler Tablo 2. 3'te sunulmuştur.

Tablo 2.3. *Araştırma uygulama katılımcıları*

		Kadın	Kadın %	Erkek	Erkek %	Toplam	Toplam %
Yaş Aralığı		18-39	-	18-37	-	18-39	-
Fakülte	Edebiyat Fakültesi	110	75,9	35	24,1	145	9,1
	Eğitim Fakültesi	205	72,2	79	27,8	284	17,8
	İktisadi ve İdari Bilimler Fakültesi	73	55,3	59	44,7	132	8,3
	Mühendislik Fakültesi	30	33	61	67	91	5,7
	İletişim Fakültesi	133	47,3	148	52,7	281	17,6
	Fen Fakültesi	112	75,2	37	24,8	149	9,3
	Turizm Fakültesi	77	47,2	86	52,8	163	10,2
	Hukuk Fakültesi	118	66,3	60	33,7	178	11,2
	Eczacılık Fakültesi	116	67,1	57	32,9	173	10,8
Toplam		974	61	622	39	1596	100
Sınıf Düzeyi	1. sınıf	209	64,7	114	35,3	323	20,3
	2. sınıf	317	59,8	213	40,2	530	33,3
	3. sınıf	266	63,5	153	36,5	419	26,3
	4. sınıf	146	57,5	108	42,5	254	16
	Hazırlık	2	66,7	1	33,3	3	0,2
	Diğer	33	53,2	29	46,8	62	3,9
Toplam		973	61,2	618	38,8	1591	100,0
İnternet Kullanım Durumu	0-1 yıl	3	100,0	0	0	3	0,2
	2-3 yıl	21	77,8	6	22,2	27	1,7
	4-5 yıl	106	71,6	42	28,4	148	9,3
	6-7 yıl	292	73,6	105	26,4	397	25
	8 yıl ve üstü	545	53,9	466	46,1	1011	63,7
Toplam		967	61	619	39	1586	100
İnternet Kullanım Sıklığı	Haftada 0-2 saat	9	56,3	7	43,8	16	1
	Haftada 2-5 saat	24	60	16	40	40	2,5
	Günde 0-2 saat	120	55,3	97	44,7	217	13,7
	Günde 3-5 saat	468	62,4	282	37,6	750	47,2
	Günde 5-7 saat	318	64,9	172	35,1	490	30,9
	Diğer	32	42,7	43	57,3	75	4,7
Toplam		971	61,1	617	38,9	1588	100,0
İnternet Erişim Araçları	Akıllı telefon	972	61,5	608	38,5	1580	-
	Tablet	97	57,1	73	42,9	170	-
	Bilgisayar	750	58,3	537	41,7	1287	-
	Diğer (Bknz. Tablo 3.4)	6	24	19	76	25	-
İnternet Kullanım Amaçları	Çevrimiçi oyunlar	185	33,7	364	66,3	549	-
	Film, video vb. izleme	926	60,8	597	39,2	1523	-
	Dosya indirme	704	59,1	488	40,9	1192	-
	Araştırma yapma	886	61,6	553	38,4	1439	-
	İletişim kurma	922	62,3	557	37,7	1479	-
	Haber okuma	714	57,1	536	42,9	1250	-
	Diğer	77	4,8	46	2,9	123	-

Tablo 2. 3'teki katılımcıların öğrenim gördükleri fakülteler incelendiğinde, en fazla Eğitim Fakültesi 284 (%17,8) ve onu takiben İletişim Fakültesi 281 (%17,6), en az ise Mühendislik Fakültesi 91 (0%5,7) öğrencisinden veri elde edilmiştir. Araştırma katılımcıları çeşitli sınıf düzeylerindedir. Hazırlık ve lisansüstü eğitim, ikinci üniversite gibi diğer kategorisinde ele alınan düzeyler haricinde en az 4. sınıf düzeyinde 254 (%16) katılımcıya ulaşılmıştır. İnternet kullanım durumları açısından bakıldığında araştırma katılımcılarının büyük bir çoğunluğu 1011 (63,7) sekiz yıl ve üzeri süredir internet kullandığı görülmüştür. Bunun yanında katılımcıların büyük çoğunluğu 750 (%47,2) günde 3-5 saat, 490 (%30,9)'ı ise günde 5-7 saat aralığında internet kullandığını belirtmişlerdir. Kullanım sıklığını haftalık oranlarda açıklayan katılımcı sayısı ise oldukça azdır. Araştırma katılımcılarının internete erişimi sağlayan araçları incelendiğinde kadın katılımcıların 972 (61,5)'si, erkek katılımcıların 608 (38,5)'inin akıllı telefonlar, kadın katılımcıların 750 (58,3)'si ve erkek katılımcıların 537 (41,7)'sinin kişisel bilgisayarları aracılığıyla internete erişim sağladıkları görülmüştür. Katılımcılar en fazla film, video vb. izleme ve iletişim kurma, en az ise diğer kategorisi haricinde çevrimiçi oyun oynama amacıyla internet kullandıklarını belirtmişlerdir. Araştırma katılımcılarının internet erişimi kurduğu diğer kategorisinde bulunan araçlar ve internet kullanım amaçları Tablo 2. 4'te sunulmuştur.

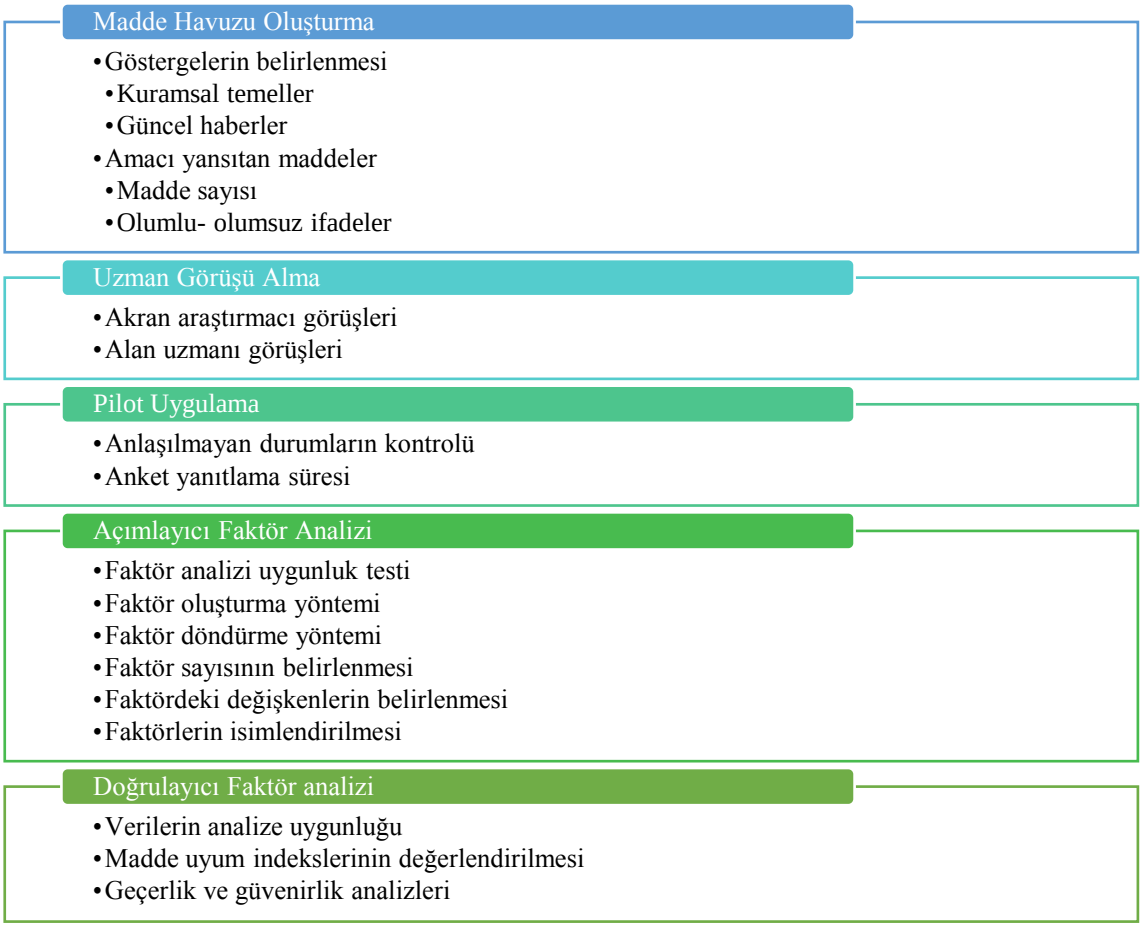
Tablo 2.4. *Araştırma katılımcılarının diğer internet erişimi kurduğu araçlar ve internet kullanım amaçları*

		Kadın (f)	**Erkek (f)**	**Toplam (f)**
İnternet erişimi kurdukları diğer araçlar	Akıllı TV	4	10	13
	Oyun konsolu (Playstation vb.)	1	7	8
	Bazı kameralar (Dronlar vb.)	0	1	1
Diğer internet kullanım amaçları	18+ yaş üstü içerik	0	2	2
	Alışveriş	7	8	15
	Sosyal medya kullanma (Sosyalleşme, paylaşımda bulunma, başkalarıyla iletişim kurma vb.)	48	19	67
	Eğitim (Dil öğrenme, ders çalışma, uzaktan eğitim, ödev yapma, araştırma, kendini geliştirme vb.)	16	8	24
	Bankacılık işlemleri	2	0	2
	İş gereği	1	6	7
	Eğlence (oyun oynama, müzik dinleme, zaman geçirme, hobileri takip etme vb.)	17	10	27
	Stlaklamak	1	0	1

Katılımcıların internet erişimi kurdukları diğer dijital araçlar arasında Tablo 2. 4'te görüldüğü gibi Akıllı TV, oyun konsolları ve bazı kameralar yer almaktadır. Bunun yanında katılımcılar, diğer internet kullanım amacı kategorisinde en fazla sosyal medya kullanma, eğlence ve eğitim amacıyla en az ise stalklama, bankacılık işlemleri ve 18+ içeriklere ulaşma gibi çeşitli internet kullanım amaçları olduğunu da belirtmişlerdir.

2.3. Veri Toplama Araçlarının Geliştirilmesi

Çalışma kapsamında Dijital Güvenlik Öz Yeterlik (DGÖY) ve Çevrimiçi Risk Alma Eğilimi (ÇRAE) ölçekleri geliştirilmiştir. Veri toplama araçları geliştirmede madde havuzunu oluşturma, uzman görüşü alma gibi Şekil 2.1'de belirtilmiş aşamalar izlenirken, bu aşamalar içerisindeki Şekil 2.2'de belirtilmiş alt basamaklara dikkat edilmiştir.



Şekil 2.2. *Veri toplama araçları geliştirilirken izlenen alt aşamalar*

Bu bölümde Şekil 2.2'de görülen ve aday DGÖY ve ÇRAE ölçekleri için ayrı ayrı ele alınan alt aşamalar ele alınmıştır.

2.4. Aday DGÖY ölçeğinin geliştirilmesi

Aday DGÖY ölçeğinin geliştirilmesinde Şekil 2.2'te belirtilen alt aşamalar izlenmiş ve bu bağlamda yapılan çalışmalar bu bölümde sunulmuştur.

Şekil 2.3. *Ölçek geliştirme süreci*

Aday ölçek geliştirilirken DeVellis (2012)'in veri toplama aracı geliştirme sürecinden yararlanarak Şekil 2.3'te belirtilen madde havuzu oluşturma, uzman görüşünün alınması, pilot uygulamanın gerçekleştirilmesi ve geçerlik ve güvenirlik çalışmaları kapsamında Açımlayıcı Faktör Analizi (AFA) ve Doğrulayıcı Faktör Analizi (DFA) aşamaları izlenmiştir.

2.4.1. Aday DGÖY ölçeğinin madde havuzunun oluşturulması

Aday DGÖY ölçeğinin madde havuzu oluşturulurken, ölçek maddelerinin yazımı, anlam ve kapsamlarının kontrol edilmesi, düzenlenmesi ve gruplanması, danışman görüşünün alınması ve maddelere son halinin verilmesi aşamaları izlenmiştir. İlgili tarihlerde tez izleme komitesinde bulunan jüri üyeleri tarafından yapılan inceleme sonucunda madde havuzu 35 maddeden oluşturulmuştur.

Dijital güvenlik öz yeterliği göstergelerinin neler olduğunun belirlenmesi için öncelikle literatür taraması gerçekleştirilmiştir. 21. yy. becerileri, dijital yeterlikler, dijital güvenlik becerileri ve dijital okuryazarlık ile ilgili gerçekleştirilen taramada dijital güvenlik becerilerinin özel olarak ele alınmadığı görülmüştür. Ayrıca dijital güvenlik becerileri denildiğinde sadece teknolojik araçların teknik özellikleri dikkate alınarak söz konusu teknolojik araç merkezli güvenlik tedbirlerine odaklanılmıştır. Gün geçtikçe hem teknolojik araçların teknik özelliklerini hem bu araçlarla kullanılan ve her geçen gün yenilenen uygulamaların özelliklerini bilmenin ve kişinin dijital ortamlardaki varlıklarını ve dijital araçlarındaki bilgi ve belge güvenliklerini sağlama konusunda dijital güvenliği sağlama becerileri önem kazanmıştır. Bu doğrultuda yapılan taramalarda, uygulamalarda güvenlik, gezinimde güvenlik ve erişimde güvenlik olmak üzere üç yeterlik alanı ortaya çıkmıştır. İlgili yeterlik alanlarını yansıtan göstergeler ise Tablo 2.5'te sunulmuştur.

Tablo 2.5. *Aday DGÖY ölçeğinin yeterlik alanları ve göstergeleri*

Yeterlik Alanı	Göstergeler
Uygulamalarda Güvenlik	• Gizlilik ve güvenlik ayarlarını yapılandırabilmek • Bilgi ve belgelere erişim izinlerini yönetebilmek • Paylaşım izinlerini yönetebilmek • Güncelleme izinlerini yönetebilmek • Engelleme özelliklerini kullanabilmek • Uyarı özelliklerini işe koşabilmek
Gezinimde Güvenlik	• Gezinim geçmişini temizleyebilmek • Tarayıcı gizlilik ve güvenlik ayarlarını yapılandırabilmek • Gezinim modlarını kullanabilmek • Güvenli servis sağlayıcıları seçebilmek • Çoklu doğrulama tekniklerini kullanabilmek • İçerik engelleyebilmek, silebilmek veya görüntü alabilmek • Servis sağlayıcısına rapor gönderebilmek
Erişimde Güvenlik	• Güçlü şifre oluşturabilmek • Verileri yedekleyebilmek • Antivirüs ve filtreleme programı kullanabilmek • Yazılım güncellemelerini yönetebilmek • Güvenlik duvarını aktifleştirebilmek • Üyelik silebilmek • Aygıt takip ayarı yapabilmek • Hesaplardan güvenli çıkış yapabilmek

İlgili alanyazın taranması sonucunda Tablo 2.5'te belirtilen göstergeler çerçevesinde madde havuzu oluşturulmuştur. Oluşturulan 51 madde bir alan uzmanı ile birlikte tekrarlı çalışmalarla değerlendirilmiştir. Bu çalışmalarda tekrara düşülen maddeler, maddelerdeki anlam bozuklukları, maddelerin açık ve netliği ve maddelerin karmaşık olup olmadıkları kontrol edilmiştir. Bu bağlamda madde havuzunda çeşitli düzeltmeler yapılmıştır (Ek 1). Aday DGÖY ölçeğinin bu yapısı tez izleme komite üyeleri tarafından incelenmiş, maddelere ilişkin dönütler verilmiştir. Aday ölçeğin maddeleri için önerilen bu düzeltmeler yapıldıktan sonra üç akran araştırmacı ve tez danışmanı ile birlikte maddeler üzerinde incelemeler gerçekleştirilmiştir. Daha sonra aday DGÖY ölçeği için uzman görüşü alma aşamasına geçilmiştir.

2.4.2. Aday DGÖY ölçeğinin madde havuzu için uzman görüşüne başvurulması

Aday DGÖY ölçeği madde havuzu için sekiz akran araştırmacı ve sekiz alan uzmanının görüşlerine başvurulmuştur. Akran araştırmacıların her birinin dönütleri incelenmiş, alınan her dönütten sonra ölçek maddeleri üzerinde yeni düzeltmeler yapılmıştır. Bu aşamadan sonra aday DGÖY ölçek maddeleri hakkında sekiz alan uzmanının görüşlerine başvurulmuştur. Uzmanlar düzeltilmesi gerekenler maddelerin üzerine eksik ya da anlaşılmayan hususları belirtmişlerdir. Bu doğrultuda alan uzmanların

her birinin dönütleri incelenmiş ve önerdikleri düzeltmeler gerçekleştirilmiştir. Akran araştırmacılar ve alan uzmanlarının görüşleri doğrultusunda, ölçülmek istenilen yapıların kapsamı, içerdikleri terminoloji ve anlaşılabilir olup olmadıkları değerlendirilmiştir. Örneğin "SMS kodu, güvenlik sorusu gibi güvenlik kodu kullanmadan internetten alışveriş yapmak" şeklinde yazılan bir maddeye, bir akran araştırmacı tarafından "Güvenlik kodu değil de güvenlik önlemi denilebilir." şeklinde terminolojik bir dönüt verilmiştir. Başka bir örnek olarak da "Doğruluğundan emin olmadığım bilgileri çevrimiçi ortamlarda paylaşmak" maddesine ilişkin "Doğruluğundan emin olmak daha çok bilgi okuryazarlığını ölçen bir maddeye doğru gidiyor. Çıkartılmalı ya da risk alma bağlamında düzenlenmeli." şeklinde ölçülmek istenilen yapı kapsamının değerlendirildiği bir dönüt verilmiştir. Nihai aday DGÖY ölçeği toplam 35 maddeden oluşturulan yapıya dönüştürülmüştür (Ek 2). Son olarak aday DGÖY ölçeği dilbilgisi alan uzmanı tarafından incelenmiş ve herhangi bir dilbilgisi kuralı bakımından düzeltmeye gerek duyulmamıştır.

Aday DGÖY ölçeğinin uzman görüşü aşamasında Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE) Anabilim Dalı'ndan sekiz uzmanın ve aynı anabilim dalında doktora düzeyindeki sekiz akran araştırmacının görüşü alınmıştır. Uzmanlar, internet çocuk ve aile, güvenli internet kullanımı ve bilişim teknolojileri alanlarında çeşitli bilimsel araştırmalar ve projeler yürütmüşlerdir. Aynı zamanda bu uzmanlar uzmanlık alanları kapsamında çeşitli ölçme araçları geliştirmişlerdir. Akran araştırmacılar ise bilişim teknolojileri, dijital vatandaşlık, internet ve etik, dijital bilgelik, güvenli internet kullanımı alanlarında bilimsel araştırmalara katılmış ve bu alandaki çeşitli bilimsel projelerde görev almışlardır. Uzman ve akran araştırmacıların görüşleri doğrultusunda aday DGÖY ölçeği üzerinde gerçekleştirilen düzeltmelerden sonra, Türkçe Eğitimi Bölümü'nde öğretim üyesi olan bir uzman da dilbilgisi, anlam ve noktalama işaretleri bakımından ilgili ölçeği kontrol etmiştir. Bu aşamada aday DGÖY ölçeğinin yüz görünüş geçerliği tamamlanmıştır.

2.4.3. Aday DGÖY ölçeğinin pilot uygulaması

Aday DGÖY ölçeğinin pilot uygulaması çeşitli 4 yıllık fakülte ve bölümlerde örgün öğrenim gören 19 üniversite öğrencisi ile gerçekleştirilmiştir. Bu üniversite öğrencilerinin özellikleri Tablo 2.6'da görülmektedir.

Tablo 2.6. *Aday DGÖY ölçeğinin pilot uygulama katılımcı özellikleri*

Cinsiyet	Yaş	Fakülte	Bölüm	Öğrenim düzeyi	İnternet Kullanım süresi	İnternet Kullanım sıklığı
Erkek	23	Mühendislik Fakültesi	Bilgisayar Mühendisliği	2. sınıf	6-7 yıl	Günde 5-7 saat
Kadın	24	Mühendislik Fakültesi	Bilgisayar Mühendisliği	4. sınıf	6-7 yıl	Günde 5-7 saat
Erkek	21	Mühendislik Fakültesi	Bilgisayar Mühendisliği	3. sınıf	8 yıl ve üzeri	Günde 3-5 saat
Erkek	20	Mühendislik Fakültesi	Bilgisayar Mühendisliği	2. sınıf	6-7 yıl	Günde 3-5 saat
Kadın	21	Eğitim Fakültesi	BÖTE	3. sınıf	6-7 yıl	Günde 5-7 saat
Erkek	23	Eğitim Fakültesi	İşitme Engelliler Öğretmenliği	4. sınıf	6-7 yıl	Günde 5-7 saat
Kadın	21	Eğitim Fakültesi	İşitme Engelliler Öğretmenliği	4. sınıf	8 yıl ve üzeri	Günde 0-2 saat
Erkek	21	Eğitim Fakültesi	Sınıf Öğretmenliği	4. sınıf	6-7 yıl	Günde 0-2 saat
Erkek	22	Eğitim Fakültesi	Sınıf Öğretmenliği	4. sınıf	8 yıl ve üzeri	Günde 10 saat
Erkek	-	Eğitim Fakültesi	Sınıf Öğretmenliği	4. Sınıf	6-7 yıl	Günde 0-2 saat
Kadın	20	Eğitim Fakültesi	İngilizce Öğretmenliği	2. sınıf	6-7 yıl	Günde 0-2 saat
Kadın	25	Edebiyat Fakültesi	Arkeoloji	4. sınıf	6-7 yıl	Günde 3-5 saat
Erkek	28	Edebiyat Fakültesi	Arkeoloji	Yüksek Lisans	4-5 yıl	Günde 3-5 saat
Kadın	26	Edebiyat Fakültesi	Arkeoloji	Yüksek Lisans	8 yıl ve üzeri	Günde 5-7 saat
Kadın	25	Fen Fakültesi	Biyoloji	4. sınıf	8 yıl ve üzeri	Günde 3-5 saat
Kadın	23	Fen Fakültesi	Biyoloji	4. sınıf	8 yıl ve üzeri	Günde 3-5 saat
Kadın	24	Fen Fakültesi	Biyoloji	4. sınıf	6-7 yıl	Günde 3-5 saat
Kadın	24	İletişim Bilimleri Fakültesi	Basın ve Yayın	4. sınıf	8 yıl ve üzeri	Günde 3-5 saat
Kadın	22	Eğitim Fakültesi	İngilizce Öğretmenliği	2. sınıf	8 yıl ve üzeri	Günde 3-5 saat

Tablo 2.6'da görüldüğü gibi aday DGÖY ölçeğinin pilot uygulama katılımcılarının sekizi erkek, on biri kadındır. Katılımcılar 20-28 yaş aralığında olup, hepsi en az 4-5 yıldır internet kullanıcısıdır. Aday DGÖY ölçeğinin uygulanacağı hedef kitlenin ölçek maddelerinde anlamadıkları hususları belirlemek, ölçeğin kaç dakikada yanıtlandığını belirlemek için farklı fakültelerin çeşitli bölümlerinde öğrenim gören 19 üniversite öğrencisi ile pilot uygulama gerçekleştirilmiştir. Pilot uygulama ile aday veri toplama aracının yanıtlanma süresinin 15-30 dakika aralığında değiştiği görülmüştür. Veri

toplama aracının demografik bilgiler bölümünde tekrar eden bir soru tespit edilmiş ve ölçek formundan çıkartılmıştır.

2.4.4. Aday DGÖY ölçeğinin AFA aşaması katılımcıları

Araştırmanın evrenini Eskişehir ili devlet üniversitelerinin 4 yıllık fakültelerinde örgün öğrenim gören üniversite öğrencileri oluşturmaktadır. AFA aşaması için hedef evreni temsil etmesi ve araştırma verilerinin toplandığı aşamalarda aynı öğrencilerden veri toplamayı engellemek amacıyla araştırma evreni ve katılımcıları başlığında belirtilen Tablo 2.1'de yer alan Anadolu Üniversitesi'nde, 2000'in üzerinde öğrenci sayısına sahip, dört farklı fakülteden veri toplanmıştır. İktisadi ve İdari Bilimler Fakültesi, Eğitim Fakültesi, Mühendislik Fakültesi ve Edebiyat Fakültesi'nden toplamda 500 katılımcıdan veri toplanmıştır. AFA aşaması verileri toplanırken araştırmanın bu sürecine katılan ve sonra ilgili ölçek maddelerinin bir kısmına yanıt vermek istemeyen 10 katılımcının verileri çalışma dışında bırakılmıştır. Bu doğrultuda aday DGÖY ölçeğinin AFA çalışmaları için 490 üniversite öğrencisine ait veriler kullanılmıştır.

Veri setinin faktör analizi için uygunluğunun test edilmesi amacıyla ilk olarak örneklem büyüklüğüne bakılmıştır. Tabachnick ve Fidell (2007) korelasyon matrisinin güvenilir sonuçlar vermesi için örneklem büyüklüğünün 300'ün üzerinde olması gerektiğini belirtmektedir. Comrey ve Lee (1992)'ye göre 1000 katılımcı faktör analizi için mükemmel kabul edilmektedir. Bu doğrultuda mevcut veri setinin (n=490) AFA için uygun büyüklükte olduğu sonucuna varılmıştır. Verilerin faktör analizi için uygunluğunun test edilmesi amacıyla Barlett küresellik testi sonucuna bakılmış, sonuç anlamlı bulunmuştur ($\chi 2(595) = 11738{,}450$; $p < .001$). Ancak Barlett küresellik testi örneklem büyüklüğüne duyarlı olduğu için büyük örneklemlerde yanıltıcı sonuçlar verebilmektedir (Tabachnick ve Fidell, 2007). Böyle durumlarda veri setinin faktör analizi için uygunluğunun test edilmesi için farklı kanıtlar sunulması gerektiği belirtilmektedir (Worthington ve Whittaker, 2006). Bu doğrultuda örneklem büyüklüğü açısından veri yapısının faktör analizi için uygunluğunu test etmek için Kaiser-Mayer-Olkin (KMO) değeri hesaplanmış, bulunan .968 değerinin iyi bir faktör analizi için önerilen minimum değer olan .6'nın çok üstünde olduğu görülmüştür (Tabachnick ve Fidell, 2007). Aday DGÖY ölçeğinin AFA aşaması için 490 katılımcıya ilişkin demografik özellikler Tablo 3.7'de görülmektedir.

Tablo 2.7. *Aday DGÖY ölçeğinin AFA aşaması katılımcı bilgileri*

		Kadın	Kadın %	Erkek	Erkek %	Toplam	Toplam %
Yaş Aralığı		16-30	-	18-31	-	-	-
Fakülte	Edebiyat Fakültesi	102	35,1	29	14,6	131	26,7
	Eğitim Fakültesi	80	27,5	48	24,1	128	26,1
	İktisadi ve İdari Bilimler Fakültesi	62	21,3	59	29,6	121	24,7
	Mühendislik Fakültesi	47	16,2	63	31,7	110	22,4
Toplam		291	100	199	100	490	100
Sınıf	1. sınıf	57	19,6	46	23,1	103	21,0
Düzeyi	2. sınıf	96	33,0	99	49,7	195	39,8
	3. sınıf	107	36,8	41	20,6	148	30,2
	4. sınıf	27	9,3	11	5,5	38	7,8
	Hazırlık	0	0,0	1	0,5	1	,2
	Diğer	3	1,0	1	0,5	4	,8
Toplam		291	100	199	100	490	100
İnternet	0-1 yıl	0	0,0	0	0,0	0	-
Kullanım	2-3 yıl	5	1,7	1	0,5	6	1,2
Durumu	4-5 yıl	32	11,0	17	8,5	49	10,0
	6-7 yıl	91	31,3	44	22,1	135	27,6
	8 yıl ve üstü	162	55,7	136	68,3	298	60,8
Toplam		291	100	199	100	490	100
İnternet	Haftada 0-2 saat	9	3,1	1	0,5	10	2,0
Kullanım	Haftada 2-5 saat	2	0,7	5	2,5	7	1,4
Sıklığı	Günde 0-2 saat	38	13,1	36	18,1	74	15,1
	Günde 3-5 saat	142	48,8	80	40,2	222	45,3
	Günde 5-7 saat	97	33,3	61	30,7	158	32,2
	Diğer	1	0,3	14	7,0	15	3,1
Toplam		291	100	199	100	490	100

Tablo 2.7'de görüldüğü üzere aday DGÖY ölçeği AFA katılımcılarının 291'i (%59,4) kadın, 199'u (%40,6) ise erkek üniversite öğrencileridir. Kadın katılımcıların yaşları 16-30, erkek öğrencilerin ise 18-31 aralığındadır. Katılımcıların öğrenim gördükleri fakülteler incelendiğinde en fazla kadın katılımcının (%35,1) Edebiyat Fakültesi, en az kadın katılımcının (%16,2) ise Mühendislik Fakültesi'nde öğrenim gördüğü, en fazla erkek katılımcının (%31,7) Mühendislik Fakültesi, en az erkek katılımcının (%14,6) ise Edebiyat Fakültesi'nde öğrenim gördüğü görülmektedir. Sınıf düzeyleri bakımından en fazla katılımcının 2. Sınıf düzeyi 195 (%39,8), onu takip eden en fazla katılımcının ise 3. Sınıf düzeyi 148 (%30,2) olduğu görülmektedir. Katılımcıların internet kullanım durumlarına bakıldığında kadın katılımcıların 162 (%55,7)'si ve erkek katılımcıların 136 (%68,3)'ü 8 yıldan fazla süredir internet kullanıcısı olduğu, katılımcıların 6 (%1,2)'sının ise 2-3 yıldır internet kullandığı dikkat çekmektedir. İnternet kullanım sıklıkları bakımından katılımcıların 222 (%45,3)'si günde 3-5 saat aralığında

İnterneti kullandıklarını belirtirken 7 (%1,4)'sinin haftada 2-5 saat aralığında İnternet kullandıkları görülmektedir.

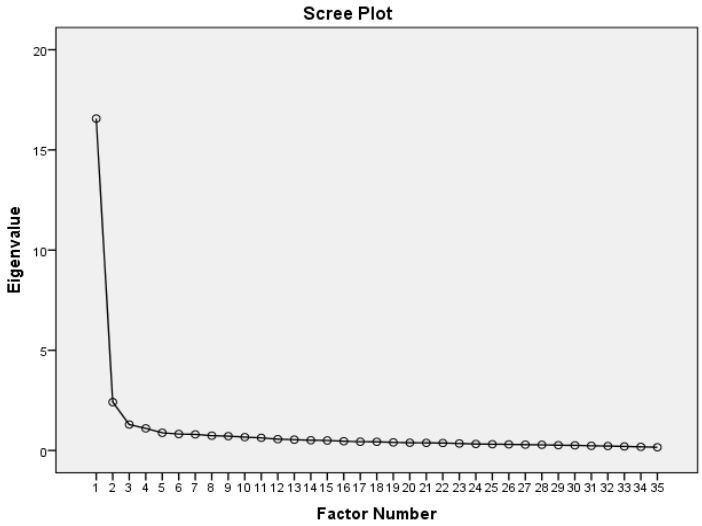
2.4.5. Aday DGÖY ölçeğinin AFA süreci

Pilot çalışma tamamlandıktan sonra aday DGÖY ölçeğinin AFA aşamasına geçilmiştir. Eskişehir ili devlet üniversitelerinin dört yıllık örgün öğretim veren fakültelerinde veri toplamak amaçlanmıştır. Bu doğrultuda Anadolu Üniversitesi Etik Kurulu'ndan izini (Ek 3) alınmıştır. Bu iznin ardından Anadolu Üniversitesi'nden (Ek 4) ve Eskişehir Osmangazi Üniversitesi'nden araştırma uygulama izinleri alınmıştır (Ek 5) alınmıştır.

Aday Dijital Güvenlik Öz Yeterlik (DGÖY) ölçeğinin örtük değişkenlerini ortaya çıkarmak ve yapı geçerliğini sağlamak amacıyla açımlayıcı faktör analizi (AFA) gerçekleştirilmiştir. Analize başlanmadan önce veri seti, kayıp değerler için kontrol edilmiş, değişken sayısının (n=35) yarısı ve üzerinde kayıp değeri olan veriye rastlanmamıştır. Bu işlemden sonra kalan kayıp değerlerin analizi etkileme durumunu kontrol altına almak amacıyla bu değerler, seri ortalamaları ile doldurulmuştur (Çokluk, Şekercioğlu ve Büyüköztürk, 2014). Daha sonra örtük değişkenlerin normallikleri incelenmiş ve maksimum çarpıklık (S) değerinin I-2,307I ve maksimum basıklık (K) değerinin I5,321I olduğu ve Kline (2015) basıklık ve çarpıklık değerlerine göre veri setinin normal dağılım gösterdiği kabul edilmiştir. Aday DGÖY ölçeğinin AFA aşaması kapsamında Anadolu Üniversitesindeki 2000 üstü öğrenci sayısına sahip dört farklı fakülteden 490 adet veri toplanmıştır. Aday DGÖY ölçeğin faktör analizi için uygunluğu test edildiğinde Bartlett Küresellik testinin sonucu anlamlı ve KMO değeri .968 bulunmuştur. Bu doğrultuda verilerin, AFA'ne tabi tutulmak için uygun olduğu görülmüştür.

Faktör çıkarım amacıyla temel bileşenler (principal component analysis) faktör analizi kullanılmıştır. Böylece maddeler arasında paylaşılan varyansı açıklayan gizil değişkenleri bulmak amaçlanmıştır (Worthington ve Whittaker, 2006). Gerçekleştirilen faktör analizinde veri setindeki değişkenler arası çoklu bağlantı problem yarattığı için korelasyon matrisi incelenmiş ve .90 üstü korelasyona sahip değişken bulunmadığı görülmüştür (Field, 2009). Verilerin döndürülmesinde; değişkenlerin faktörlerdeki yüklerinin varyansını arttırarak faktör yapısını basitleştirmek, böylece kolay yorumlanabilir bir yapı ortaya koymak amacıyla dik (orthogonal) döndürme

işlemlerinden Varimax tercih edilmiştir (Tabachnick ve Fidell, 2007). Korunacak faktör sayısının belirlenmesi için ilk olarak, Kaiser ölçütü ele alınmıştır. Kaiser ölçütü, örneklem sayısının 250'nin üstünde ve ortalama ortak varyans (communality) değerlerinin 0.6'nın üstünde olduğu durumlarda özdeğeri 1'in üzerinde olan tüm faktörlerin korunmasını önermektedir (Field, 2009). Analiz sonuçları özdeğeri 1'in üzerinde olan 4 faktör bulunduğunu göstermiştir. Mevcut örneklemde Kaiser ölçütünün uygulanabilmesi için gerekli olan 250 üzeri katılımcı şartı sağlanmış, ancak ortak varyans (communality) değerleri ortalaması 0,59 olduğu görülmüş, bu nedenle bu ölçüt faktör belirlemede dikkate alınmamıştır.



Şekil 2.4. *Catell's yamaç-birikinti grafiği*

Korunacak faktör sayısını belirlemek amacıyla Şekil 2.4'teki yamaç-birikinti (scree plot) grafiği incelenmiş, bu doğrultuda ilk keskin kırılmanın 2. faktörde gerçekleştiği görülmüştür. Stevens (2000)'a göre 200'den büyük örneklemlerde yamaç-birikinti grafiği oldukça güvenilir sonuçlar vermektedir. Ancak yamaç-birikinti grafiğinin tek başına faktör belirlemede yeterli olamayacağı belirtilmektedir (Field, 2009). Henson ve Roberts (2006) da faktör belirlerken birden fazla stratejinin işe koşulmasını önermektedir. Huck (2012), özdeğeri toplam özdeğerin %5'inden fazla olan faktörlerin korunması ölçütünü faktör belirleme stratejilerinden biri olarak değerlendirmektedir. Bu bağlamda özdeğerler toplamının %5'i 1,7 olarak hesaplanmış; özdeğeri 1,75'in üzerinde olan iki faktör bulunduğu tespit edilmiştir. Yamaç-birikinti grafiği ve %5 kriteri sonucunda iki faktörlü bir yapı ile AFA gerçekleştirilmesine karar verilmiştir. Maddelerin ölçekte tutulması için

faktör yükü alt sınırı .40 olarak belirlenmiştir. Ayrıca maddelerin iki faktörde gösterdikleri yükler farkı için .10 değeri esas alınmıştır. Tabachnick ve Fidell (2007) düşük ortak varyans değerlerine sahip maddelerin veri setindeki diğer maddelerle ilişkisiz olarak değerlendirilebileceğini belirtmektedir. Worthington ve Whittaker (2006) maddelerin faktörlerin açıkladıkları varyansa katkısının göstergesi olan ortak varyans değerlerinin maddelerin ölçekte tutulması için önemli bir değerlendirme aracı olduğunu belirtmektedir. Bu doğrultuda düşük ortak varyans değerleri (<.04) madde çıkarılmasında bir kriter olarak değerlendirilmiştir. Tablo 2.8'de aday DGÖY ölçeğinin faktör yapısı sunulmuştur.

Tablo 2.8. *Aday DGÖY ölçeğinin faktör yapısı*

Faktörler ve Maddeler	**Açıklanan varyans (%)**	**$\bar{x}$**	**Ss**	**Madde Toplam r**	**Faktör Yükü**
Faktör 1: Çevrimiçi Uygulamalarda Güvenlik (α=,939)					
17. Çevrimiçi alışveriş …		4,38	1,004	,725	,810
27. Çevrimiçi hesaplarım …		4,49	,851	,731	,804
13. Cep No bilgimi kullanan …		4,45	,962	,665	,795
24. İstenmeyen arkadaşlık …		4,50	,916	,613	,785
3. Çevrimiçi hesaplarıma …		4,42	,977	,703	,763
1. Facebook, Instagram gibi …	31,138	4,28	1,021	,647	,751
28. Çevrimiçi uygulamaların …		4,34	,949	,731	,742
21. Dijital hesaplarıma …		4,22	1,032	,726	,682
15. Çevrimiçi uygulamaların, …		4,16	1,004	,711	,674
18. Çevrimiçi uygulama …		4,20	1,035	,655	,664
5. Cep No bilgimi kullanan …		4,15	1,054	,680	,657
Faktör 2: Dijital Araçlarda Güvenlik (α=,906)					
7. Dijital araçlarımın …		3,34	1,169	,518	,725
34. İnternet erişimi …		3,64	1,105	,540	,698
9. Sabit disk, …		3,59	1,162	,549	,696
30. Dijital araçlarımdaki …		3,87	1,093	,682	,692
10. Ağ bağlantımı …		3,66	1,167	,616	,691
22. İnternet erişiminde …	25,683	3,85	1,086	,694	,645
23. İnternette gezinirken …		3,85	1,077	,614	,638
6. Web tarayıcıma …		3,74	1,121	,653	,617
4. Dijital araçlarımda …		3,54	1,170	,554	,614
35. İnternet tarayıcımın …		4,00	1,082	,744	,602
26. Ağ bağlantımı …		4,03	1,078	,627	,563
12. İstenmeyen reklam …		3,87	1,125	,548	,520
Toplam (α=,947)	56,821				

Madde faktör yükleri ilgili faktör altında .40'ı geçen ve bulaşık madde özelliği göstermeyen üç madde, faktörel isimlendirmenin yapılabilmesi için bulundukları faktörler altında yorumlanamamışlardır. Bu üç maddenin ayrı ayrı ve hepsinin aday analiz

dışında bırakılmasıyla aday DGÖY ölçeğinin yapısındaki değişiklikler incelenmiştir. Bu incelemeler doğrultusunda her iki faktörde bulunan maddeler arasında değişiklik olmadığı belirlenmiş ve ilgili üç maddenin ölçek yapısından çıkartılması uygun bulunmuştur. Tablo 2.8'de görüldüğü üzere elde edilen 2 faktörlü yapıda 1. faktör altında bulunan ve yükleri .65-.81 arasında değişen 11 madde ile varyansın %31.138'i, 2. faktör altında bulunan ve yükleri .52-.75 arasında değişen 12 madde ile varyansın %25,683'ü açıklanmıştır. 2 faktörlü yapı ile açıklanan toplam %56,821 varyans, sosyal bilimler alanında gerçekleştirilen çalışmalar için yeterli kabul edilmektedir (Scherer vd., 1988; akt. Çokluk, Şekercioğlu ve Büyüköztürk, 2014). Buna ek olarak ölçeğin güvenirlik katsayısı .947 olup, yüksek güvenirliğe sahip olduğu söylenebilmektedir (Özdamar, 2004).

Verilerin analizi sonucunda Tablo 2.8'de görülen iki faktörlü yapının isimlendirilmesinde faktörlerde bulunan maddeler temel alınmıştır. Faktör 1'in altında yer alan maddeler incelendiğinde ortak noktanın çevrimiçi uygulamalarda gerçekleştirilen işlemler çerçevesinde toplandığı görülmüştür. Bu nedenle Faktör 1, "Çevrimiçi Uygulamalarda Güvenlik" olarak isimlendirilmiştir. Faktör 2'nin altında yer alan maddeler incelendiğinde ise ortak noktanın dijital araçlarda gerçekleştirilebilen güvenlik önlemleri çerçevesinde toplandığı görülmüştür. Bu nedenle Faktör 2, "Dijital Araçlarda Güvenlik" olarak isimlendirilmiştir. Geliştirilen aday DGÖY ölçeği formu yorumlanabilir yapıdadır. Aynı zamanda kuramsal yapıyla da oldukça uyumludur.

2.4.6. Aday DGÖY ölçeğinin DFA aşaması katılımcıları

Aday DGÖY ölçeğinin DFA aşaması için hedef evreni temsil etmesi ve araştırma verilerinin toplandığı aşamalarda aynı öğrencilerden veri toplamayı engellemek amacıyla araştırma evreni ve katılımcıları başlığında belirtilen Tablo 2.1'de yer alan Eskişehir Osmangazi Üniversitesi'nde, 2000'in üzerinde öğrenci sayısına sahip, dört farklı fakülteden veri toplanmıştır. Mühendislik Fakültesi, Fen Edebiyat Fakültesi, İktisadi ve İdari Bilimler Fakültesi ve Eğitim Fakültesi'nde öğrenim gören 1193 katılımcıdan veri toplanmıştır. Elde edilen veriler incelenmiş ve ilgili ölçeğe hepsini aynı puan (hepsi 5, hepsi 1 vb.) girmiş, desen oluşturarak işaretleme yapmış ve maddelerin yarısından fazlasını boş bırakmış 372 katılımcının verileri DFA aşamasında değerlendirmeye alınmamıştır. Bu doğrultuda aday DGÖY ölçeğinin DFA çalışmaları için 821 katılımcıya ait veriler kullanılmıştır. Bu aşamadaki veriler AFA aşamasında kullanılan verilerden

farklıdır. Çünkü ölçek geliştirmenin AFA sürecinde değişkenlerin birbirleri arasındaki ilişkiler dikkate alınmaktadır (Wothington ve Wihittaker, 2006), DFA aşamasında ise AFA sonucunda faktörel olarak ulaşılan ölçek yapısının söz konusu örneklemde test edilmesi amaçlanmaktadır. Yani değişkenler arasında AFA sonucu ortaya çıkmış olan ilişkilerin doğrulanıp doğrulanmadığına bakılır. Ölçek geliştirme süreci DFA aşamasında kullanılan örneklem büyüklüğü için aday ölçekteki madde sayısı temel alınabilir. Wothington ve Wihittaker (2006) her madde için minimum beş, ideal olarak ise her madde için on katılımcı sayısına ulaşılmasını önermektedir. Kline (2012) ise 100 ile 200 arasındaki katılımcı sayısına ulaşılmasını önermiştir. Bu anlamda analize tabi tutulan 821 katılımcıdan edinilen veri seti DFA için uygun büyüklüktedir ve bu katılımcılara ilişkin ayrıntılı bilgi ve özellikler Tablo 2.9'da görülmektedir.

Tablo 2.9. *Aday DGÖY ölçeğinin DFA aşaması katılımcı bilgileri*

		Kadın	Kadın %	Erkek	Erkek %	Toplam	Toplam %
Yaş Aralığı		18-35	-	18-44	-	-	-
Fakülte	Fen Edebiyat Fakültesi	84	19,9	43	10,9	127	15,5
	Eğitim Fakültesi	166	39,3	61	15,5	227	27,6
	İktisadi ve İdari Bilimler Fakültesi	126	29,9	105	26,6	231	28,1
	Mühendislik Fakültesi	46	10,9	105	26,6	231	28,1
Toplam		422	100	394	100	821	100
Sınıf Düzeyi	1. sınıf	171	40,6	137	34,9	308	37,5
	2. sınıf	83	19,7	67	17,0	150	18,3
	3. sınıf	97	23,0	85	21,6	182	22,2
	4. sınıf	58	13,8	82	20,9	140	17,1
	Hazırlık	2	0,5	0	0,0	2	0,2
	Diğer	10	2,4	22	5,6	32	3,9
Toplam		421	100	393	100	821	100
İnternet Kullanım Durumu	0-1 yıl	1	0,2	-	-	1	0,1
	2-3 yıl	7	1,7	5	1,3	12	1,5
	4-5 yıl	60	14,3	32	8,2	92	11,2
	6-7 yıl	120	28,5	81	20,7	201	24,5
	8 yıl ve üstü	233	55,3	273	69,8	506	61,6
Toplam		421	100	391	100	821	100
İnternet Kullanım Sıklığı	Haftada 0-2 saat	4	1,0	-	-	4	0,5
	Haftada 2-5 saat	12	2,9	11	2,8	23	2,8
	Günde 0-2 saat	47	11,2	60	15,4	107	13,0
	Günde 3-5 saat	197	46,9	176	45,2	373	45,4
	Günde 5-7 saat	150	35,7	126	32,4	276	33,6
	Diğer	10	2,4	16	4,1	26	3,2
Toplam		420	100	389	100	821	100

Aday DGÖY ölçeğinin DFA aşamasında analize tabi tutulan 821 katılımcının 422 (%51,4)'si kadın, 395 (%48,1)'i erkek üniversite öğrencilerinden oluşmaktadır.

Katılımcılardan 4 (%0,5)'ü ise cinsiyet bilgisini belirtmemiştir. Tablo 2.9'da DFA aşaması için yanıt veren kadın katılımcıların yaş aralıkları 18-35, erkek katılımcıların ise 18-44'tür. Katılımcıların öğrenim gördükleri fakülteler incelendiğinde en fazla kadın katılımcının (%39,3) Eğitim Fakültesi, en az kadın katılımcının (%10,9) ise Mühendislik Fakültesi'nde öğrenim gördüğü, erkek katılımcıların ise en fazla Mühendislik Fakültesi (%26,6) ve İktisadi ve İdari Bilimler Fakültesi'nde (%26,6), en az erkek katılımcının (%10,9) ise Fen Edebiyat Fakültesi'nde öğrenim gördüğü görülmektedir.

Tablo 2.9 sınıf düzeyi bakımından incelendiğinde, en fazla katılımcının (%37,5) 1. sınıf, onu takiben de en fazla katılımcının (%22,2)3. sınıf düzeyinde olduğu görülmektedir. Katılımcıların internet kullanım durumları incelendiğinde en fazla katılımcının (%61,6) 8 yıl ve üstü süredir internet kullanıcısı olduğu, sadece bir katılımcının ise bir yıldır internet kullanıcısı olduğu dikkat çekmektedir. İnternet kullanım sıklığı açısından bakıldığında en fazla katılımcının (%45,4) günde 3-5 saat aralığında internet kullandığı, onu takip eden en fazla katılımcının (%33,6) ise günde 5-7 saat aralığında İnternet kullandığı görülmektedir.

2.4.7. Aday DGÖY ölçeği DFA süreci

Doğrulayıcı faktör analizi (DFA) daha önceden oluşturulmuş bir modelin, doğrulanıp, doğrulanmadığını sınayan bir analizdir (Çokluk, Şekercioğlu ve Büyüköztürk, 2012). AFA sonuçlarına göre elde edilen modelin, yapı geçerliğini değerlendirmek amacıyla DFA'ya başvurulmuştur (Kline, 2015). Aday DGÖY ölçeği AFA sonucunda 23 maddeli (Ek 6) iki faktörlü yapıya ulaşılmıştır. Aday DGÖY ölçeğinin DFA aşaması için Eskişehir Osmangazi Üniversitesi 2000 üstü öğrenci sayısına sahip dört farklı fakülteden veri toplanmış, DFA'da 821 kişilik veri seti analiz edilmiştir.

Bu çalışmada 23 gözlenen değişken ile 2 gizil değişkene ilişkin bir ölçme modeli oluşturulmuştur. Model uyumu değerlendirilirken kritik indeksler olarak Tablo 2.10'da belirtilen; $\chi 2/sd$ (ki-kare/serbestlik derecesi), yaklaşık hataların ortalama karekökü (RMSEA), standardize edilmiş ortalama hataların karekökü (SRMR), normlaştırılmış uyum indeksi (NFI), normlaştırılmamış uyum indeksi (NNFI) ve karşılaştırmalı uyum indeksi (CFI) göz önünde bulundurulmuştur. İki faktörlü ölçme modeli için 821 kişilik veri seti ile hiçbir düzeltme gerçekleştirilmeden elde edilen DFA sonucunda ulaşılan uyum iyiliği indeksleri [$\chi 2/sd=5.53$ $p<.01$; RMSEA= .07; CFI=.95; NFI= .94; NNFI=.95; SRMR=.05] olarak bulunmuştur.

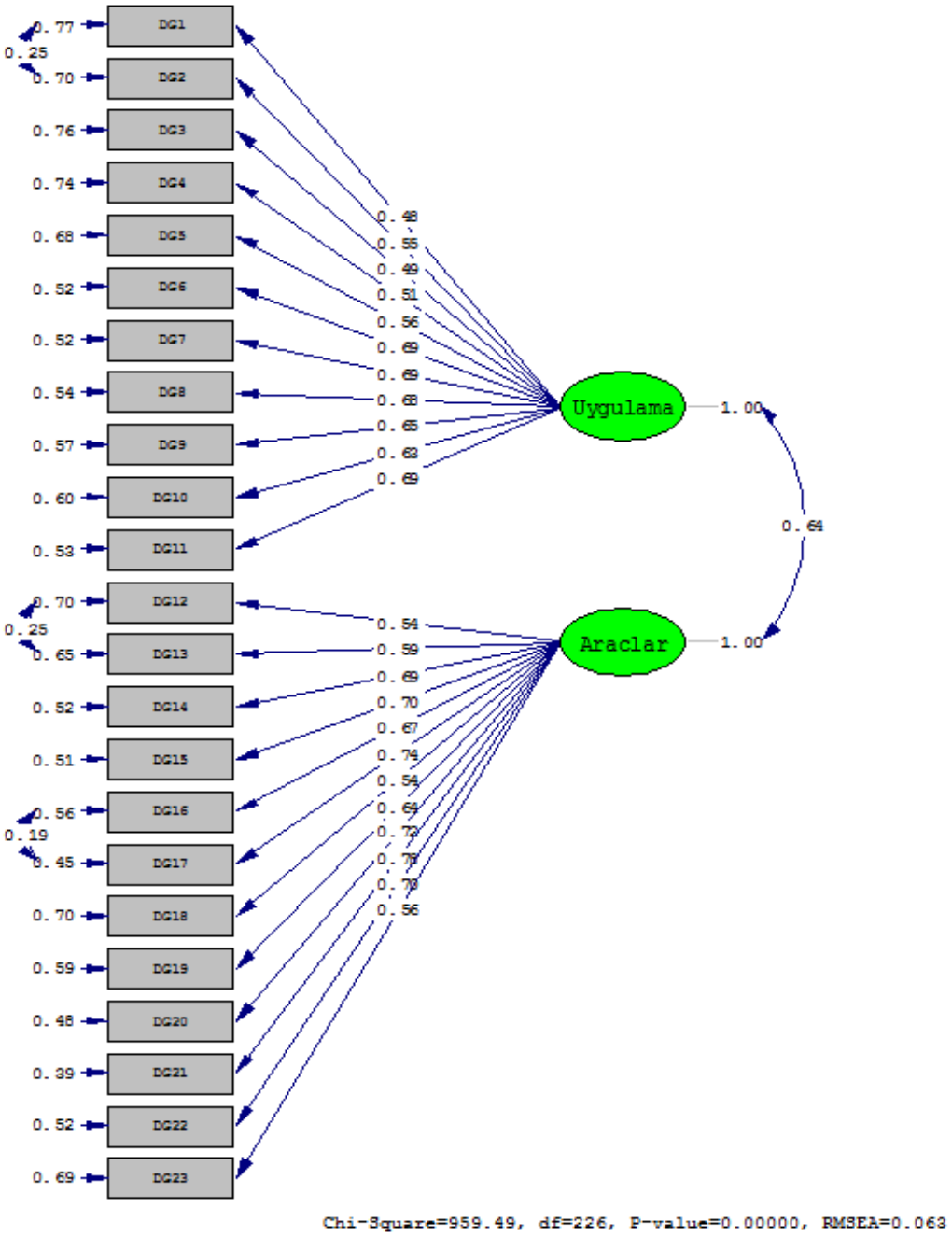
Tablo 2.10. *Model Uyum İndeksleri*

Uyum İndeksi	İyi Uyum Değeri	Kabul Edilebilir Uyum Değeri	Kaynak
χ^2	$0 \leq \chi^2 \leq 2sd$	$2sd < \chi^2 \leq 3sd$	(Tabachnick ve Fidell, 2012)
p değeri	$.05 \leq p \leq 1.00$	$.01 \leq p \leq .05$	(Hoyle, 1995)
χ^2/sd	$0 \leq \chi^2/sd \leq 2$	$2 \leq \chi^2/sd \leq 3$	(Schermelleh-Engel, Moosbrugger ve Müller, 2003)
		$2 \leq \chi^2/sd \leq 5$	(Wheaton, Muthen, Alwin, ve Summers, 1977, s. 99; Marsh ve Hocevar, 1985, s. 576; Kelloway, 1998 (Akt. Erkorkmaz, Etikan, Demir, Özdamar ve Sanisoğlu, 2013))
RMSEA	$0 \leq RMSEA \leq .05$	$.05 \leq RMSEA \leq .08$	(Browne ve Cudeck, 1992; Hu ve Bentler, 1999, s. 27; Schreiber, Nora, Stage, Barlow ve King, 2006)
SRMR	$0 \leq SRMR \leq .05$	$.05 \leq SRMR \leq .10$	(Hu ve Bentler, 1999, s. 27)
NFI	$.95 \leq NFI \leq 1.00$	$.90 \leq NFI < .95$	(Schermelleh-Engel, Moosbrugger ve Müller, 2003; Tabachnick ve Fidell, 2012)
NNFI	$.97 \leq NNFI \leq 1.00$	$.95 \leq NNFI < .97$	(Hu ve Bentler, 1999, s. 27)
CFI	$.97 \leq CFI \leq 1.00$	$.95 \leq CFI < .97$	(Hu ve Bentler, 1999, s. 27; Tabachnick ve Fidell, 2012)

Bu analiz sonucunda DG2-DG1, DG13-DG12 ve DG17-DG16 maddeleri arasında üç düzeltme incelenmiş ve bu maddeler arasında tanımlanacak ilişkilerin χ2 değerini en çok düşüren değerler olduğu belirlenmiştir. Aynı zamanda bu düzeltmeler kuramsal olarak ele alındığında maddelerin benzer durumları ölçtükleri ve aralarındaki gizil ilişkilerin kabul edilebileceği düşünülmüştür. Bu doğrultuda ilgili maddeler arasında ilişkiler tanımlanmıştır. Geliştirilen dijital güvenlik öz yeterlik ölçeğinin iki faktörlü yapısına ilişkin düzenlenen yol diyagramı Şekil 2.5'da ve ölçme modelinin uyum istatistiklerinin iyileştirilmiş hali Tablo 2.11'de sunulmuştur.

Model uyumu değerlendirilirken çıkarımsal değerlendirme için χ2 testi, betimsel değerlendirmeler için ise genel uyum ölçütleri, model karşılaştırmalarına dayalı ölçütler ve model benzetimi ile ilgili ölçütler kullanılmaktadır (Schumacker ve Lomax, 1996, s. 119). DFA sonucunda çıkarımsal olarak anlamsız sonuç vermesi gereken χ2 testi büyük örnekleme sahip çalışmalarda anlamlı çıktığı görülmektedir. Bunun nedeninin ise hesaplanan χ2 değerinin örneklem sayısından oldukça fazla etkilendiği ve kovaryans matrislerinde tahmin edilen ve gözlenen değerler arasındaki önemsiz farkların anlamlı çıkması olarak belirtilmektedir (Çelik ve Yılmaz, 2013; Fan, Thompson ve Wang, 1999; Floyd ve Wideman, 1995; Lomax ve Schumacker, 2010, s. 86; Ullman ve Bentler, 2012, s. 671; Wheaton, Muthen, Alwin ve Summers, 1977, s. 99). Tablo 2.11'de görülen ve istatistiksel açıdan anlamlı olan p değeri (<.001) dikkate alınmadan model uyumu değerlendirilmiştir. Serbestlik derecesi (sd)'nin χ2 testinde önemli bir ölçüt olması, uyum ölçütlerinde χ2/sd oranının değerlendirilmesinin uygun bir uyum belirtisi olarak kabul edilmesine sebep olmaktadır (Kelloway, 1998 (Akt. Erkorkmaz vd., 2013); Schermelleh-

Engel, Moosbrugger ve Müller, 2003; Wheaton, Muthen, Alwin ve Summers, 1977, s. 99).



Şekil 2.5. *Geliştirilen dijital güvenlik öz yeterlik ölçeği DFA'ne ilişkin düzenlenen yol diyagramı (Standartlaştırılmış Değerler)*

Bunun yanında Lomax ve Schumacker, (2010, s. 91) model uyum iyiliği indeksleri değerlendirilirken χ2, RMSEA, SRMR indekslerinin her durumda rapor edilmesi gerektiğini belirtmiştir. Bu doğrultuda Tablo 2.11'de χ2 değerine de yer verilmiştir.

Tablo 2.11. *Geliştirilen dijital güvenlik öz yeterlik ölçeğinin DFA sonucunda elde edilen uyum değerleri (n=821)*

Uyum İndeksi	İyi Uyum Değeri	Kabul Edilebilir Uyum Değeri	Gözlenen Uyum Değeri	Değerlendirme
χ^2	$0 \leq \chi^2 \leq 2sd$	$2sd \leq \chi^2 \leq 3sd$	959.49>678	-
p değeri	.05≤p≤1.00	.01 ≤p≤ .05	.000	-
χ^2/sd	0≤ /sd≤2	$2 \leq \chi^2/sd \leq 5$	4.24	Kabul edilebilir uyum
RMSEA	0≤RMSEA≤.05	.05≤RMSEA≤.08	.063	Kabul edilebilir uyum
SRMR	0≤SRMR≤.05	.05≤SRMR≤.10	.050	Kabul edilebilir uyum
NFI	.95≤NFI≤1.00	.90≤NFI<.95	.961	İyi uyum
NNFI	.97≤NNFI≤1.00	.95≤NNFI<.97	.966	Kabul edilebilir uyum
CFI	.97≤CFI≤1.00	.95≤CFI<.97	.970	İyi uyum
χ^2=959.49; sd=226				

Ölçme modeline ilişkin Tablo 2.11'deki uyum indeksleri incelendiğinde değerlerin genel olarak kabul edilebilir değerler aralığında olduğu görülmektedir. Schermelleh-Engel, Moosbrugger ve Müller (2003), modelde gözlenen χ2/sd değerinin 3 ve 3'ün altında olması, modelin kabul edilebilir bir uyum göstergesine sahip olduğunu belirtirken, Wheaton, Muthen, Alwin ve Summers (1977, s. 99)'a göre bu oranın 5 veya 5'in altında olması yeterlidir. Dolayısıyla, Tablo 2'de belirtilen χ2/sd=4.24 değeri, kabul edilebilir bir uyum değeri olarak ele alınabilir. Hu ve Bentler (1999, s. 27) ve Browne ve Cudeck (1992, s. 239), RMSEA uyum indeksinin <.05 olmasını iyi uyum, <.08 olmasını ise değerlendirilebilir yani kabul edilebilir uyum olduğunu belirtmektedirler. Bu doğrultuda geliştirilen ölçeğin sahip olduğu .063 RMSEA değeri kabul edilebilir uyum değeri olarak yorumlanabilir. SRMR uyum indeksinin <.05 olması iyi uyum değeri (Lomax ve Schumacker, 2010, S. 91), <.10 olması ise kabul edilebilir uyum değeri olarak yorumlanmaktadır (Hu ve Bentler, 1999 s. 27). Dolayısıyla geliştirilen ölçeğin SRMR uyum değerinin .05 olması, kabul edilebilir uyum değerine sahip olduğunu göstermektedir. Schermelleh-Engel, Moosbrugger ve Müller (2003) ve Tabachnick ve Fidell (2012)'e göre NFI uyum indeksinin .95 ile 1.00 aralığında olması iyi uyum değeri, .90 ile .95 aralığında olması ise kabul edilebilir uyum değeri olarak yorumlanmaktadır. Bu doğrultuda geliştirilen ölçeğin sahip olduğu NFI uyum indeksinin .961 olması iyi uyuma sahip olduğunun bir göstergesi olarak kabul edilebilir. NNFI ve CFI uyum indekslerinin değerleri .97 ve 1.00 aralığında iyi uyum, .95 ile .97 aralığında ise kabul edilebilir uyum değeri olarak yorumlanmaktadır (Hu ve Bentler, 1999, S. 27; Tabachnick ve Fidell, 2012). Geliştirilen ölçeğin NNFI uyum indeks değeri .966 olduğundan kabul edilebilir uyum değerine, CFI uyum indeks değerinin .970 olması ise iyi uyum değerine

sahip olduğunun bir göstergesi olarak kabul edilebilir. Özetle ölçeğin 821 kişilik veri seti ile gerçekleştirilmiş DFA sonucuna göre, χ2/sd, RMSEA, SRMR ve NNFI değerlerinin "kabul edilebilir uyum" CFI ve NFI değerlerinin ise "iyi uyum" değer aralıklarında olduğu görülmektedir.

Floyd ve Wideman (1995, s.245), örneklem büyüklüğüne duyarlı olan ki-kare değeri sorununu aşmak için örneklemi küçük alt bölümlere ayırıp, DFA'nın tekrarlanmasını ve ek kanıt elde edilmesini önermiştir. Bu doğrultuda 821 kişilik örneklem büyüklüğüne sahip veri setinden rastgele ikişerli 300, 400 ve 500 kişilik veri setleri oluşturulmuş ve bu veri setleriyle DFA tekrarlanmıştır. İlgili örneklem büyüklüklerine ait DFA değerleri Tablo 2.12'de sunulmuştur.

Tablo 2.12. *DFA aşamasında toplanan veri setinden rastgele seçim ile oluşturulan örneklemlerin analizi sonucunda elde edilen uyum değerleri*

Uyum İndeksi	İyi Uyum	Kabul Edilebilir Uyum	Örneklem Büyüklüğü (n)	Gözlenen Değer
χ^2	$0 \leq \chi^2 \leq 2sd$	$2sd \leq \chi^2 \leq 3\ sd$	300	506.78<678
			300	492.16<678
			400	594.68<678
			400	584.39<678
			500	686.28>678
			500	674.37<678
p değeri	.05 <p ≤ 1.00	.01 ≤ p ≤ .05	300	.000
			300	.000
			400	.000
			400	.000
			500	.000
			500	.000
$\chi^2/\ sd$	$0 \leq \chi^2/\ sd \leq 2$	$2 \leq \chi^2/\ sd \leq 5$	300	2.242
			300	2.177
			400	2.631
			400	2.585
			500	3.036
			500	2.983
RMSEA	0 ≤ RMSEA ≤ .05	.05 <RMSEA ≤ .08	300	0.064
			300	0.063
			400	0.064
			400	0.063
			500	0.064
			500	0.060
SRMR	0 ≤ SRMR ≤ .05	.05 <SRMR ≤ .10	300	.057
			300	.059
			400	.057
			400	.055
			500	.055
			500	.051
NFI	.95 ≤ NFI ≤ 1.00	.90 ≤ NFI <.95	300	.944

Tablo 2.12. (Devam) *DFA aşamasında toplanan veri setinden rastgele seçim ile oluşturulan örneklemlerin analizi sonucunda elde edilen uyum değerleri*

Uyum İndeksi	İyi Uyum	Kabul Edilebilir Uyum	Örneklem Büyüklüğü (n)	Gözlenen Değer
NFI	.95 ≤ NFI ≤ 1.00	.90 ≤ NFI <.95	300	.949
			400	.949
			400	.954
			500	.957
			500	.959
NNFI	.97 ≤ NNFI ≤ 1.00	.95 ≤ NNFI <.97	300	.964
			300	.968
			400	.964
			400	.968
			500	.967
			500	.969
CFI	.97 ≤ CFI ≤ 1.00	.95 ≤ CFI <.97	300	.968
			300	.971
			400	.967
			400	.971
			500	.971
			500	.972
sd: 226				

Tablo 2.12'deki uyum değerleri incelendiğinde örneklem sayısı (n) küçüldükçe $\chi 2$ değerinin azaldığı ve $\chi 2/sd$'nin iyi uyuma yaklaştığı görülmektedir. DFA'da $\chi 2$ değerinin "Kabul edilebilir uyum" ve $\chi 2/sd$ ($2 \leq \chi 2/sd \leq 3$) "Kabul edilebilir uyum" aralığında değer aldığı görülmektedir (Schermelleh-Engel, Moosbrugger ve Müller, 2003; Tabachnick ve Fidell, 2012). RMSEA, SRMR ve NNFI değerlerinin genellikle "Kabul edilebilir uyum" (Browne ve Cudeck, 1992; Hu ve Bentler, 1999, s. 27), CFI ve NNFI değerlerinin ise "İyi uyum" (Hu ve Bentler, 1999, s. 27; Tabachnick ve Fidell, 2012) değer aralıklarında olduğu görülmektedir. Bu doğrultuda geliştirilen ölçeğin Tablo 2.11 ve Tablo 2.12'deki uyum indeks değerleri incelendiğinde oluşturulan ölçme modelinin doğrulandığı ifade edilebilir. Geliştirilen ölçeğin DFA'sına ilişkin her maddesine ait standardize çözümleme değerlerinin anlamlı olup olmadığını değerlendirmek için t değerleri incelenmiş ve bu değerlerin 13.60 ile 25.80 arasında değiştiği görülmüştür. Tüm maddeler için hesaplanan t değerleri $p<.01$ düzeyinde anlamlı bulunmuştur. Geliştirilen ölçeğin DFA sonrası elde edilen uyum indeks değerleri doğrultusunda, 23 maddelik ölçme aracının kabul edilebilir bir uyum gösterdiği aynı zamanda uygulanabilir olduğu görülmüştür.

Dijital Güvenlik Öz Yeterlik (DGÖY) ölçeğinin ölçmeye yöneldiği yapıyı ölçüp ölçmediğine ilişkin yapı geçerliği; yakınsak geçerliği (convergent validity) ve ıraksama geçerliğinin (divergent validity) bir diğer versiyonu olan ayırt edici geçerlilik

(diskriminant validity) teknikleri kullanılarak incelenmiştir. Yapı güvenirliği ve Cronbach Alfa katsayısı kullanılarak ölçme aracından elde edilen verilerin iç tutarlılık anlamındaki güvenirliği irdelenmiştir. Geliştirilen DGÖY ölçeğinin geçerlik ve güvenirlik analiz sonuçları Tablo 2.13'de belirtilmiştir.

Tablo 2.13. *DGÖY Ölçeği DFA özeti (n=821)*

Değişkenler	$\bar{X}$	SS	Faktör Ortalamaları	SS	Alpha Güvenirliği	Yapısal Güvenirlik	Ortalama Açıklanan Varyans	Madde Yükü	t değeri	Hata
Dijital Uygulamalarda Güvenlik										
DG1	4.59	.579						.564	13.60	0.26
DG2	4.62	.563						.657	16.05	0.22
DG3	4.51	.740						.571	14.17	0.41
DG4	4.84	.362						.623	14.66	0.10
DG5	4.70	.549						.547	16.55	0.21
DG6	4.68	.520	4.59	0.39	.84	0.86	0.37	.674	21.64	0.14
DG7	4.53	.666						.604	21.59	0.23
DG8	4.61	.595						.668	21.09	0.19
DG9	4.46	.766						.596	20.02	0.34
DG10	4.46	.741						.532	19.06	0.33
DG11	4.54	.651						.628	21.34	0.32
Dijital Araçlarda Güvenlik										
DG12	3.79	1.000						.539	16.56	0.70
DG13	3.86	1.016						.606	17.82	0.67
DG14	3.81	1.119						.718	21.82	0.65
DG15	3.90	1.068						.710	22.08	0.59
DG16	3.96	1.044						.716	20.71	0.61
DG17	3.99	1.015	3.93	0.70	.90	0.91	0.45	.753	23.88	0.47
DG18	4.07	.913						.535	16.17	0.59
DG19	3.84	.970						.637	19.91	0.55
DG20	3.72	1.050						.727	23.15	0.53
DG21	4.06	.945						.761	25.80	0.35
DG22	4.10	.977						.712	21.99	0.49
DG23	4.13	1.042						.566	16.75	0.74
Açıklanan varyans: %45.266										

Tablo 2.13 incelendiğinde ölçek boyutlarına ilişkin alfa ve yapısal güvenirlik değerlerinin 0.70'ten büyük olduğu görülmektedir. Nunnally ve Bernstein (1994)'a göre

ölçme sonuçlarının güvenirliğine ilişkin bir kanıt olarak, ölçeğin her bir boyutuna ilişkin alfa ve yapısal güvenirlik katsayılarının 0.70'ten büyük olması gerektiği belirtilmektedir. Yakınsak geçerlilik için çeşitli yollar mevcuttur. Bu yollar arasında faktör yüklerinin, Ortalama Açıklanan Varyans (OAV) değerlerinin ve yapısal güvenirlik değerlerinin incelenmesi yer almaktadır. Madde faktör yüklerinin .5 veya daha yüksek bir değere sahip olması özellikle .7 ve üstü bir değerin yakınsak geçerlik için daha ideal bir değer olduğu belirtilmektedir (Hair, vd., 2010, s. 679). Bu durumda öncelikle faktörleri oluşturan maddelerin faktör yükleri incelenmiş ve her bir boyuta ilişkin maddelerin faktör yüklerinin .532 ile .761 arasında değişen değerler aldıkları görülmüştür. Fornell ve Larcker (1981, s. 46) yakınsak geçerlik için OAV değerlerinin .5 ve üstü olması gerektiğini belirtmektedir. Fakat söz konusu ölçeğin boyutlarına ait OAV değerlerinin .36 ve .45 olduğu görülmektedir. Hair vd. (2010, s. 680) ölçek boyutlarının yapısal geçerlik değerlerinin .7 ve üstü olması iyi güvenirliği gösterirken, bir modelin yapı geçerliliğinin diğer göstergelerinin iyi olması koşuluyla .6 ile .7 arasındaki güvenirlik değerlerinin de kabul edilebileceği belirtilmiştir. Tablo 2.13'te görüldüğü üzere ölçek boyutlarına ilişkin yapısal güvenirlik değerlerinin .86 ile .91 olduğu görülmektedir. Bu doğrultuda faktör yükleri ve yapısal güvenirlik değerleri söz konusu ölçeğin yakınsak geçerliğinin bir kanıtı olarak gösterilebilir.

Ayırt edici geçerlilik için ilgili ölçeğin alt boyutları arasındaki korelasyon ve OAV değerlerinin karekökünden yararlanılmaktadır. Ayırt edici geçerliliğin sağlanması için ölçeğin her bir alt boyutlara ilişkin OAV değerlerinin kareköklerinin, o alt boyutun diğer alt boyutlar ile aralarındaki korelasyondan ve aynı zamanda 0.50 değerinden küçük olmaması gerekmektedir (Fornel ve Larcker, 1981, s. 46). Tablo 2.14'de DGÖY ölçeği faktörleri arasındaki korelasyon ve OAV değeri karekökleri belirtilmiştir.

Tablo 2.14. *DGÖY ölçeği faktörleri arasındaki korelasyon ve OAV değeri karekökü*

Boyutlar	**Ortalama**	**SS**	**1**	**2**
1. Dijital Uygulamalarda Güvenlik	4.59	0.39	**0.60**	
2. Dijital Araçlarda Güvenlik	3.93	0.70	0.54**	**0.66**

** 0.01 düzeyinde anlamlıdır.

Tablo 2.14 incelendiğinde, ölçeğin her iki alt boyutunun OAV değerlerinin kareköklerı, boyutlar arasındaki korelasyon değerinden ve 0.50 değerinden daha büyüktür. Bir başka ifadeyle dijital araçlarda güvenlik alt boyutunun OAV karekökü 0.60

iken bu alt boyutun diğer alt boyut ile olan korelasyonundan daha büyüktür. Bu doğrultuda ölçeğin ayırt edicilik geçerliğinin sağlandığı söylenebilir.

2.5. Aday ÇRAE ölçeğinin geliştirilmesi

Aday ÇRAE ölçeğinin geliştirilmesinde Şekil 2.2'de belirtilen alt aşamalar izlenmiş ve bu bağlamda yapılan çalışmalar bu bölümde sunulmuştur. Aday ölçek geliştirilirken DeVellis (2012)'in veri toplama aracı geliştirme sürecinden yararlanarak Şekil 2.3'te belirtilen madde havuzu oluşturma, uzman görüşünün alınması, pilot uygulamanın gerçekleştirilmesi ve geçerlik ve güvenirlik çalışmaları kapsamında Açımlayıcı Faktör Analizi (AFA) ve Doğrulayıcı Faktör Analizi (DFA) aşamaları izlenmiştir.

2.5.1. Aday ÇRAE ölçeğinin madde havuzunun oluşturulması

Aday ÇRAE ölçeğinin madde havuzu oluşturulurken, ölçek maddelerinin yazımı, anlam ve kapsamlarının kontrol edilmesi, düzenlenmesi ve gruplanması, danışman görüşünün alınması ve maddelere son halinin verilmesi aşamaları izlenmiştir. İlgili tarihlerde tez izleme komitesinde bulunan jüri üyeleri tarafından yapılan inceleme sonucunda madde havuzu 84 maddeden oluşturulmuştur.

Aday ÇRAE ölçeğinin uzman görüşü aşamasında Bilgisayar ve Öğretim Teknolojileri Eğitimi (BÖTE) Anabilim Dalı'ndan sekiz uzmanın ve aynı anabilim dalında doktora düzeyindeki sekiz akran araştırmacının görüşü alınmıştır. Uzmanlar, internet çocuk ve aile, güvenli internet kullanımı ve bilişim teknolojileri alanlarında çeşitli bilimsel araştırmalar ve projeler yürütmüşlerdir. Aynı zamanda bu uzmanlar uzmanlık alanları kapsamında çeşitli ölçme araçları geliştirmişlerdir. Akran araştırmacılar ise bilişim teknolojileri, dijital vatandaşlık, internet ve etik, dijital bilgelik, güvenli internet kullanımı alanlarında bilimsel araştırmalara katılmış ve bu alandaki çeşitli bilimsel projelerde görev almışlardır. Uzman ve akran araştırmacıların görüşleri doğrultusunda aday ÇRAE ölçeği üzerinde gerçekleştirilen düzeltmelerden sonra, Türkçe Eğitimi Bölümü'nde öğretim üyesi olan bir uzman da dilbilgisi, anlam ve noktalama işaretleri bakımından ilgili ölçeği kontrol etmiştir. Bu aşamada aday ÇRAE ölçeğinin yüz görünüş geçerliği tamamlanmıştır.

Çevrimiçi Riskler çerçevesinin belirlenmesi için öncelikle literatür taraması gerçekleştirilmiştir. Özellikle çocukların ve ergen bireylerin çevrimiçi riskli davranışlarının neler olduğu, karşılaştıkları riskli içerikler ve gerçek hayatta yaşadıkları

mağduriyetler konusunda çeşitli çalışmalar incelenmiştir. Çalışmalar çevrimiçi riskleri farklı kategorilerle ele almışlardır. Bunun yanında aynı zamanda ülkelerin genel olarak inceledikleri internet kullanımı konusundaki çalışmalarda ise yetişkin bireylerin de çeşitli riskli çevrimiçi davranışlarda bulundukları, riskli içeriklerle karşılaştıkları çalışmalar da incelenmiştir. Çevrimiçi davranışları karşısında zorluk yaşayan bireylerin çeşitli bloglar ve haber sitelerinde paylaştıkları, aynı zamanda birçok gazete ve haber yayınının da ele aldığı yaşanmış örnek olaylar incelenmiştir. Bu taramanın sonucunda kişisel bilgileri açma, ticari ilgiler, veri güvenliği, zorbalık, sosyalleşme, bilgi kirliliği, uygunsuz içerik ve sağlık olmak üzere sekiz çevrimiçi risk boyutu ortaya çıkmıştır. İlgili boyutları yansıtan göstergeler ise Tablo 2.15'te sunulmuştur.

Tablo 2.15. *Aday ÇRAE ölçeğinin yeterlik alanları ve göstergeleri*

Boyutlar	**Göstergeler**
Kişisel bilgileri açma	• Üyelik formlarını doldurmak • Kişisel özel bilgileri paylaşmak • Uygulamaların konum, bilgi ve belgelere erişmesine izin vermek • Herkese açık hesaplar oluşturmak • Hizmet koşul ve şartları doğrudan kabul etmek
Ticari ilgiler	• Çevrimiçi ortamlarda banka kart bilgileri kullanarak alışveriş yapmak • Tarayıcıların şifre, kart numarası gibi bilgileri kaydetmesine izin vermek • Çevrimiçi ortamlarda şans oyunları oynamak
Veri güvenliği	• Ücretsiz belge dosya vb. indirmek • Basit dizilime sahip şifreler oluşturmak • Umumi kullanıma açık dijital araçları kullanmak
Zorbalık	• Başkalarının çevrimiçi hesaplarını elde etmek • Başkalarına uygunsuz içerikli iletiler göndermek • Başkalarını çevrimiçi ortamlarda aşağılamak
Sosyalleşme	• Tanımadığın insanlarla tanışmak, iletişim kurmak • Çevrimiçi ortamlarda edinilen arkadaşlarla özel paylaşımlarda bulunmak • Çevrimiçi ortamlarda iletişim kurulan kişilerle gerçek hayatta görüşmek
Bilgi kirliliği	• Doğru olmayan bilgi paylaşımı • Kişiler, olaylar ve durumlarla ilgili çevrimiçi ortamlardaki bilgilere göre yargıda bulunmak
İçerik	• Çevrimiçi gezinim ve paylaşımları aileden gizlemek • Uygunsuz içerikler görüntülemek
Sağlık	• Güvenirliği kanıtlanmamış reçeteleri (Diyet, zayıflama ilacı vb.) edinmek • Fiziksek duruşa dikkat etmeden dijital araçları kullanmak • Aşırı derecede sosyal ağlar çevrimiçi oyunlar vb. kullanmak • Çevrimiçi zorbalığa veya istismara uğramak

İlgili alanyazın ve güncel örnek olayların taranması sonucunda Tablo 2.15'te belirtilen göstergeler çerçevesinde madde havuzu oluşturulmuştur. Oluşturulan 84 madde bir alan uzmanı ile birlikte tekrarlı çalışmalarla değerlendirilmiştir. Bu çalışmalarda tekrara düşülen maddeler, maddelerdeki anlam bozuklukları, maddelerin açık ve netliği ve maddelerin karmaşık olup olmadıkları kontrol edilmiştir. Bu bağlamda madde havuzunda çeşitli düzeltmeler yapılmıştır (Ek 2). Aday ÇRAE ölçeğinin bu yapısı tez izleme komite üyeleri tarafından incelenmiş, maddelerin fiillerine ilişkin dönütler verilmiştir. Aday ölçeğin yapısı ve maddeleri için önerilen bu düzeltmeler yapıldıktan sonra üç akran araştırmacı ve tez danışmanı ile birlikte maddeler üzerinde incelemeler gerçekleştirilmiştir. ÇRAE ölçeğinin yapısı, sağlık, tehlikeli sporlar, finans gibi farklı alalara özgü gerçek yaşam durumlarında risk alma davranışının ölçüldüğü Nicholson, Soane, Fenton-O'Creeyy ve Willman (2005) tarafından geliştirilen ve Tablo 2.16'da görülen "Risk Alma İndeksi" dikkate alınarak geliştirilmiştir.

Tablo 2.16. *Risk alma indeksi*

Risk Alanları	Şimdi					Geçmişte				
a. Eğlence riskleri (tüplü dalış yapma, yüksek dağa tırmanma vb.)	1	2	3	4	5	1	2	3	4	5
b. Sağlık riskleri (sigara içme, yüksek alkol tüketimi vb.)	1	2	3	4	5	1	2	3	4	5
c. Kariyer riskleri (başka bir iş bulmadan varolan işten çıkma vb.)	1	2	3	4	5	1	2	3	4	5
d. Finansal riskler (kumar oynama, riskli yatırımlar vb.)	1	2	3	4	5	1	2	3	4	5
e. Güvenlik riskleri (hızlı araba kullanma vb.)	1	2	3	4	5	1	2	3	4	5
f. Sosyal riskler (halka açık bir kural veya karara itiraz etmek vb.)	1	2	3	4	5	1	2	3	4	5

Tablo 2.16'da görüldüğü üzere, ilgili indekste alanlara ayrılan risk türleri, yakın geçmiş ve şimdiki zamana göre katılımcılar tarafından değerlendirilmiştir. Maddelerin yanıtlarında ise "1=Asla, 2=Nadiren, 3=Oldukça Sık, 4=Sık Sık, 5=Çok Sık" ifadelerine karşılık gelecek şeklinde puanlama yapılmıştır. Daha sonra aday ÇRAE ölçeği için uzman görüşü alma aşamasına geçilmiştir.

2.5.2. Aday ÇRAE ölçeği için uzman görüşüne başvurulması

Aday ÇRAE ölçeği madde havuzu için sekiz akran araştırmacı ve sekiz alan uzmanının görüşlerine başvurulmuştur. Akran araştırmacıların her birinin dönütleri incelenmiş, alınan her dönütten sonra ölçek maddeleri üzerinde yeni düzeltmeler yapılmıştır. Bu aşamadan sonra aday ÇRAE ölçek maddeleri hakkında sekiz alan

uzmanının görüşlerine başvurulmuştur. Uzmanlar genellikle düzeltilmesi gereken maddeler hakkında eksik ya da anlaşılmayan hususları belirtmiştir. Akran araştırmacılar ve alan uzmanlarının görüşleri doğrultusunda, ölçülmek istenilen yapıların kapsamı, içerdikleri terminoloji ve anlaşılabilir olup olmadıkları değerlendirilmiştir. Örneğin "Rahatsız edici mesaj, paylaşım, yorum veya e-postaları silebilirim." şeklinde yazılan bir maddeye, bir alan uzmanı tarafından "Platform bağımlı işlemlerden söz ediliyor. Bölünmesi ve platformların netleştirilmesi gerekli." şeklinde maddenin anlaşılırlığı için bir dönüt verilmiştir. Başka bir örnek olarak da "Çevrimiçi uygulamaların kendi hesabımda yerime paylaşım yapma izinlerini kontrol edebilirim" maddesine ilişkin ""Kendi hesabımda" öbeği çıkartılabilir. Yerine paylaşım yapması yeterli." şeklinde terminolojinin değerlendirildiği bir dönüt verilmiştir. Bu doğrultuda alan uzmanların her birinin dönütleri incelenmiş ve önerdikleri düzeltmeler gerçekleştirilmiştir. Nihai aday ÇRAE ölçeği toplam 50 maddeden oluşturulan yapıya dönüştürülmüştür (Ek 2). Son olarak aday ÇRAE ölçeği dilbilgisi alan uzmanı tarafından incelenmiş ve herhangi bir dilbilgisi kuralı bakımından düzeltmeye gerek duyulmamıştır.

2.5.3. Aday ÇRAE ölçeğinin pilot uygulama süreci

Aday ÇRAE ölçeğinin pilot uygulaması çeşitli dört yıllık fakülte ve bölümlerde örgün öğrenim gören 19 üniversite öğrencisi ile gerçekleştirilmiştir. Bu üniversite öğrencilerinin özellikleri Tablo 2.17'de görülmektedir.

Tablo 2.17. *Aday ÇRAE ölçeğinin pilot uygulama katılımcı özellikleri*

Cinsiyet	Yaş	Fakülte	Bölüm	Öğrenim düzeyi	İnternet Kullanım süresi	İnternet Kullanım sıklığı
Erkek	23	Mühendislik Fakültesi	Bilgisayar Mühendisliği	2. sınıf	6-7 yıl	Günde 5-7 saat
Kadın	24	Mühendislik Fakültesi	Bilgisayar Mühendisliği	4. sınıf	6-7 yıl	Günde 5-7 saat
Erkek	21	Mühendislik Fakültesi	Bilgisayar Mühendisliği	3. sınıf	8 yıl ve üzeri	Günde 3-5 saat
Erkek	20	Mühendislik Fakültesi	Bilgisayar Mühendisliği	2. sınıf	6-7 yıl	Günde 3-5 saat
Kadın	21	Eğitim Fakültesi	BÖTE	3. sınıf	6-7 yıl	Günde 5-7 saat
Erkek	23	Eğitim Fakültesi	İşitme Engelliler Öğretmenliği	4. sınıf	6-7 yıl	Günde 5-7 saat
Kadın	21	Eğitim Fakültesi	İşitme Engelliler Öğretmenliği	4. sınıf	8 yıl ve üzeri	Günde 0-2 saat
Erkek	21	Eğitim Fakültesi	Sınıf Öğretmenliği	4. sınıf	6-7 yıl	Günde 0-2 saat

Tablo 2.17. (Devam) *Aday ÇRAE ölçeğinin pilot uygulama katılımcı özellikleri*

Cinsiyet	Yaş	Fakülte	Bölüm	Öğrenim düzeyi	İnternet Kullanım süresi	İnternet Kullanım sıklığı
Erkek	22	Eğitim Fakültesi	Sınıf Öğretmenliği	4. sınıf	8 yıl ve üzeri	Günde 10 saat
Erkek	-	Eğitim Fakültesi	Sınıf Öğretmenliği	4. Sınıf	6-7 yıl	Günde 0-2 saat
Kadın	20	Eğitim Fakültesi	İngilizce Öğretmenliği	2. sınıf	6-7 yıl	Günde 0-2 saat
Kadın	25	Edebiyat Fakültesi	Arkeoloji	4. sınıf	6-7 yıl	Günde 3-5 saat
Erkek	28	Edebiyat Fakültesi	Arkeoloji	Yüksek Lisans	4-5 yıl	Günde 3-5 saat
Kadın	26	Edebiyat Fakültesi	Arkeoloji	Yüksek Lisans	8 yıl ve üzeri	Günde 5-7 saat
Kadın	25	Fen Fakültesi	Biyoloji	4. sınıf	8 yıl ve üzeri	Günde 3-5 saat
Kadın	23	Fen Fakültesi	Biyoloji	4. sınıf	8 yıl ve üzeri	Günde 3-5 saat
Kadın	24	Fen Fakültesi	Biyoloji	4. sınıf	6-7 yıl	Günde 3-5 saat
Kadın	24	İletişim Bilimleri Fakültesi	Basın ve Yayın	4. sınıf	8 yıl ve üzeri	Günde 3-5 saat
Kadın	22	Eğitim Fakültesi	İngilizce Öğretmenliği	2. sınıf	8 yıl ve üzeri	Günde 3-5 saat

Tablo 2.17'de görüldüğü üzere, aday ÇRAE ölçeğinin pilot uygulama katılımcılarının sekizi erkek, on biri kadındır. Katılımcılar 20-28 yaş aralığında olup, hepsi en az 4-5 yıldır internet kullanıcısıdır. Aday ÇRAE ölçeğinin uygulanacağı hedef kitlenin ölçek maddelerinde anlamadıkları hususları belirlemek, ölçeğin kaç dakikada yanıtlandığını belirlemek için farklı fakültelerin çeşitli bölümlerinde öğrenim gören 19 üniversite öğrencisi ile pilot uygulama gerçekleştirilmiştir. Pilot uygulama ile aday veri toplama aracının yanıtlanma süresinin 15-30 dakika aralığında değiştiği görülmüştür. Veri toplama aracının demografik bilgiler bölümünde tekrar eden bir soru tespit edilmiş ve ölçek formundan çıkartılmıştır.

2.5.4. Aday ÇRAE ölçeğinin AFA aşaması katılımcıları

Araştırmanın evrenini Eskişehir ili devlet üniversitelerinin dört yıllık fakültelerinde örgün öğrenim gören üniversite öğrencileri oluşturmaktadır. AFA aşaması için hedef evreni temsil etmesi ve araştırma verilerinin toplandığı aşamalarda aynı öğrencilerden veri toplamayı engellemek amacıyla araştırma evreni ve katılımcıları başlığında belirtilen Tablo 3.1'de alan Anadolu Üniversitesi'nde, 2000'in üzerinde öğrenci sayısına sahip, dört farklı fakülteden veri toplanmıştır. İktisadi ve İdari Bilimler Fakültesi, Eğitim

Fakültesi, Mühendislik Fakültesi ve Edebiyat Fakültesi'nden toplamda 500 katılımcıdan veri toplanmıştır. AFA aşaması verileri toplanırken araştırmanın bu sürecine katılan ve sonra ilgili ölçek maddelerinin bir kısmına yanıt vermek istemeyen 10 katılımcının verileri çalışma dışında bırakılmıştır. Bu doğrultuda aday ÇRAE ölçeğinin AFA çalışmaları için 490 üniversite öğrencisine ait veriler kullanılmıştır.

Veri setinin faktör analizi için uygunluğunun test edilmesi amacıyla ilk olarak örneklem büyüklüğüne bakılmıştır. Tabachnick ve Fidell (2007) korelasyon matrisinin güvenilir sonuçlar vermesi için örneklem büyüklüğünün 300'ün üzerinde olması gerektiğini belirtmektedir. Comrey ve Lee (1992)'ye göre 1000 katılımcı faktör analizi için mükemmel kabul edilmektedir. Bu doğrultuda mevcut veri setinin (n=490) AFA için uygun büyüklükte olduğu sonucuna varılmıştır. Verilerin faktör analizi için uygunluğunun test edilmesi amacıyla Barlett küresellik testi sonucuna bakılmış, sonuç anlamlı bulunmuştur ($\chi 2(378) = 3767{,}147$; $p<.001$). Ancak Barlett küresellik testi örneklem büyüklüğüne duyarlı olduğu için büyük örneklemlerde yanıltıcı sonuçlar verebilmektedir (Tabachnick ve Fidell, 2007). Böyle durumlarda veri setinin faktör analizi için uygunluğunun test edilmesi için farklı kanıtlar sunulması gerektiği belirtilmektedir (Worthington ve Whittaker, 2006). Bu doğrultuda örneklem büyüklüğü açısından veri yapısının faktör analizi için uygunluğunu test etmek için Kaiser-Mayer-Olkin (KMO) değeri hesaplanmış, bulunan .915 değerinin iyi bir faktör analizi için önerilen minimum değer olan .6'nın çok üstünde olduğu görülmüştür (Tabachnick ve Fidell, 2007). Aday ÇRAE ölçeğinin AFA aşaması için 490 katılımcıya ilişkin ayrıntılı bilgi ve özellikler Tablo 2.7'de görülmektedir.

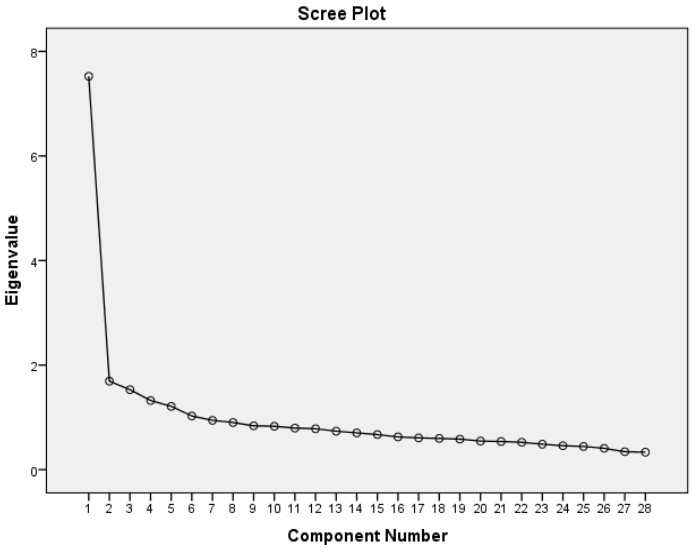
2.5.5. Aday ÇRAE ölçeği AFA süreci

Pilot çalışma tamamlandıktan sonra aday ÇRAE ölçeğinin AFA aşamasına geçilmiştir. Eskişehir ili devlet üniversitelerinin dört yıllık örgün öğretim veren fakültelerinde veri toplamak amaçlanmıştır. Bu doğrultuda Anadolu Üniversitesi Etik Kurul izni (Ek 3) alınmıştır. Bu iznin ardından, Anadolu Üniversitesi'nden (Ek 4) ve Eskişehir Osmangazi Üniversitesi'nden (Ek 5) araştırma uygulama izinleri alınmıştır. Aday ÇRAE ölçeğinin örtük değişkenlerini ortaya çıkarmak ve yapı geçerliğini sağlamak amacıyla açımlayıcı faktör analizi (AFA) gerçekleştirilmiştir. Analize başlanmadan önce veri seti, kayıp değerler için kontrol edilmiş, değişken sayısının (n=50) yarısı ve üzerinde kayıp değeri olan veriye rastlanmamıştır. Ardından kalan kayıp değerlerin analizi

etkileme durumunu kontrol altına almak amacıyla bu değerler seri ortalamaları ile doldurulmuştur (Çokluk, Şekercioğlu ve Büyüköztürk, 2014). Herhangi bir analiz işlemi yapılmadan önce ölçekte yer alan ve ters madde niteliği taşıyan maddeler (M4, M7, M10, M14, M17, M22, M32, M40, M42, M47, M49 ve M50) incelenmiş ve yeniden değer atamaları gerçekleştirilmiştir. Daha sonra örtük değişkenlerin normallikleri incelenmiş ve maksimum çarpıklık (S) değerinin I3,723I ve maksimum basıklık (K) değerinin I13,991I olduğu görülmüştür. Kline (2015)'in normal dağılım için belirttiği çarpıklık ve basıklık katsayıları dikkate alındığında ölçek maddelerinden M18, M28 ve M33'in belirtilen bu kriterlerden fazla değerlere sahip olduğu diğer örtük değişkenlerin ise maksimum çarpıklık değerinin I2,851I ve maksimum basıklık değerinin I8,082I olduğu görülmüştür. Dolayısıyla normal dağılım göstermeyen M18, M28 ve M33 örtük değişkenleri analiz dışı bırakılmıştır. Bunun dışındaki örtük değişkenlerin ise çarpıklık ve basıklık katsayıları Kline (2015)'ın çarpıklık ve basıklık katsayıları değer aralıklarına göre normal dağılım gösterdiği kabul edilmiştir. Aday ÇRAE ölçeğinin AFA aşaması kapsamında Anadolu Üniversitesindeki 2000 üstü öğrenci sayısına sahip dört farklı fakülteden 490 adet veri toplanmıştır. Veriler faktör analizine tabi tutulmadan önce ölçek maddelerinin bu ölçeğe ait olup olmadığını belirlemek için güvenirlik analizi yapılmıştır. Bu durumda ise doğrulanmış madde toplam korelasyon değerleri 0,30'dan küçük olan ve büyük olasılıkla bu ölçeğe hizmet etmeyen maddelerin (M2, M3, M4, M7, M10, M14, M17, M22, M24, M29, M32, M34, M36, M38, M40, M42, M43, M47, M48, M49, M50) açımlayıcı faktör analizinde kullanılmamasına karar verilmiştir. Aday ÇRAE ölçeğin faktör analizi için uygunluğu test edildiğinde Bartlett Küresellik testinin sonucu anlamlı ve KMO değeri .915 bulunmuştur. Bu doğrultuda verilerin, AFA için uygun olduğu görülmüştür.

Faktör çıkarım amacıyla temel bileşenler (principal component analysis) faktör analizi kullanılmıştır. Böylece maddeler arasında paylaşılan varyansı açıklayan gizil değişkenleri bulmak amaçlanmıştır (Worthington ve Whittaker, 2006). Gerçekleştirilen faktör analizinde veri setindeki değişkenler arası çoklu bağlantı problem yarattığı için korelasyon matrisi incelenmiş ve .90 üstü korelasyona sahip değişken bulunmadığı görülmüştür (Field, 2009). Verilerin döndürülmesinde; değişkenlerin faktörlerdeki yüklerinin varyansını arttırarak faktör yapısını basitleştirmek, böylece kolay yorumlanabilir bir yapı ortaya koymak amacıyla dik (orthogonal) döndürme işlemlerinden Varimax tercih edilmiştir (Tabachnick ve Fidell, 2007). Korunacak faktör sayısının belirlenmesi için ilk olarak, Kaiser ölçütü ele alınmıştır. Kaiser ölçütü, örneklem

sayısının 250'nin üstünde ve ortalama ortak varyans (communality) değerlerinin 0.6'nın üstünde olduğu durumlarda özdeğeri 1'in üzerinde olan tüm faktörlerin korunmasını önermektedir (Field, 2009). Analiz sonuçları özdeğeri 1'in üzerinde olan 6 faktör bulunduğunu göstermiştir. Mevcut örneklemde Kaiser ölçütünün uygulanabilmesi için gerekli olan 250 üzeri katılımcı şartı sağlanmış, ancak ortak varyans (communality) değerleri ortalaması 0,51 olduğu görülmüş, bu nedenle bu ölçüt faktör belirlemede dikkate alınmamıştır.



Şekil 2.2. *Catell's yamaç-birikinti grafiği*

Korunacak faktör sayısını belirlemek amacıyla Şekil 2.6'daki yamaç-birikinti (scree plot) grafiği incelenmiş, bu doğrultuda ilk keskin kırılmanın 5. faktörde gerçekleştiği görülmüştür. Stevens (2000)'a göre 200'den büyük örneklemlerde yamaç-birikinti grafiği oldukça güvenilir sonuçlar vermektedir. Ancak yamaç-birikinti grafiğinin tek başına faktör belirlemede yeterli olamayacağı belirtilmektedir (Field, 2009). Henson ve Roberts (2006) da faktör belirlerken birden fazla stratejinin işe koşulmasını önermektedir. Huck (2012), özdeğeri toplam özdeğerin %5'inden fazla olan faktörlerin korunması ölçütünü faktör belirleme stratejilerinden biri olarak değerlendirmektedir. Bu bağlamda özdeğerler toplamının %5'i 1,3 olarak hesaplanmış; özdeğeri 1,3'ün üzerinde olan 4 faktör bulunduğu tespit edilmiştir. Yamaç-birikinti grafiği ve özdeğerler toplamının %5'i kriteri sonucunda dört faktörlü bir yapı ile AFA gerçekleştirilmesine karar verilmiştir. Maddelerin ölçekte tutulması için faktör yükü alt sınırı .40 olarak

belirlenmiştir. Ayrıca maddelerin iki faktörde gösterdikleri yükler farkı için .10 değeri esas alınmıştır. Tabachnick ve Fidell (2007) düşük ortak varyans değerlerine sahip maddelerin veri setindeki diğer maddelerle ilişkisiz olarak değerlendirilebileceğini belirtmektedir. Worthington ve Whittaker (2006) maddelerin faktörlerin açıkladıkları varyansa katkısının göstergesi olan ortak varyans değerlerinin maddelerin ölçekte tutulması için önemli bir değerlendirme aracı olduğunu belirtmektedir. Bu doğrultuda düşük ortak varyans değerleri (<.04) madde çıkarılmasında bir kriter olarak değerlendirilmiştir. Tablo 2.18'de aday ÇRAE ölçeğinin faktör yapısı sunulmuştur.

Tablo 2.18. *Aday ÇRAE ölçeğinin faktör yapısı*

Faktörler ve Maddeler	**Açıklanan varyans (%)**	**x**	**Ss**	**Madde Toplam r**	**Faktör Yükü**
Faktör 1: Sosyalleşme riskleri (α=,810)					
6. İnternetten tanıştığım …	15,470	1,73	,903	,436	.714
44. Sosyal ağlarda arkadaş …		1,77	1,013	,582	.672
19. Çevrimiçi ortamlar …		1,92	1,099	,630	.670
39. İnternette tanıştığım kişilerle …		1,65	1,020	,510	.614
12. Yüz yüze tanımadığım …		2,25	1,193	,635	.586
27. Çevrimiçi ortamlarda …		1,91	0,999	,513	.538
Faktör 2: Ticari riskler (α=,657)					
16. Çevrimiçi oyunlarda …	12,466	1,60	1,125	,476	.679
31. Web siteleri üzerinden …		1,63	1,140	,528	.617
3. Alışveriş siteleriyle …		2,25	1,256	,356	.571
9. Yazılımların korsan …		1,91	1,374	,494	.539
Faktör 3: Kişisel bilgileri açma riskleri (α=,653)					
30. Çevrimiçi uygulamaların …	11,477	2,20	1,131	,420	.662
37. Messenger, WhatsApp gibi …		2,29	1,172	,377	.655
8. Özel bilgilerimi …		2,05	1,098	,480	.631
15. Çevrimiçi uygulamaların …		2,51	1,147	,358	.563
43. Ortak erişime açık …		2,86	1,224	,282	.547
Faktör 4: Başkalarına zarar verme riskleri (α=,683)					
26. Başkalarının şifrelerini …	11,236	1,31	0,775	,334	.755
20. Doğruluğundan emin …		1,40	0,797	,458	.625
11. Başkalarına müstehcenlik, …		1,35	0,861	,529	.580
5. Çevrimiçi ortamlarda …		1,41	0,830	,590	.580
Toplam (α=*,862*)	50,649				

Tablo 2.18'de görüldüğü üzere, elde edilen 4 faktörlü yapıda 1. faktör altında bulunan ve yükleri .53-.71 arasında değişen 6 madde ile varyansın %15.470'i, 2. faktör altında bulunan ve yükleri .53-.67 arasında değişen 4 madde ile varyansın %12,466'sı, 3. faktör altında bulunan ve yükleri .54-.66 arasında değişen 5 madde ile varyansın %11,477'si 4. faktör altında bulunan ve yükleri .58-.75 arasında değişen 4 madde ile

varyansın%11,236'sı açıklanmıştır. 4 faktörlü yapı ile açıklanan toplam %50,649 varyans, sosyal bilimler alanında gerçekleştirilen çalışmalar için yeterli kabul edilmektedir (Scherer ve diğerleri, 1988; akt. Çokluk, Şekercioğlu ve Büyüköztürk, 2014). Buna ek olarak ölçeğin güvenirlik katsayısı .862 olup, yüksek güvenirliğe sahip olduğu söylenebilmektedir (Özdamar, 2004).

Verilerin analizi sonucunda Tablo 2.18'de görülen dört faktörlü yapının isimlendirilmesinde faktörlerde bulunan maddeler temel alınmıştır. Faktör 1'in altında yer alan maddeler incelendiğinde ortak noktanın internet aracılığıyla edinilen arkadaşlıklarla ilgili eylemlerden oluştuğu görülmektedir. Bu nedenle Faktör 1, "Sosyalleşme Riskleri" olarak isimlendirilmiştir. Faktör 2'nin altında yer alan maddeler incelendiğinde ortak noktanın internet aracılığıyla bir ürün veya hizmeti satın alma işlemleri çerçevesindedir. Bu nedenle Faktör 2, "Ticari Riskler" olarak isimlendirilmiştir. Faktör 3'ün altındaki maddeler incelendiğinde sanal ortamlarda kişisel bilgilerin paylaşılması ve erişilmesi konusu etrafında toplanmıştır. Bu nedenle Faktör 3, "Kişisel Bilgileri Açma Riskleri" olarak isimlendirilmiştir. Faktör 4'ün altındaki maddeler incelendiğinde ise dijital araç veya ortamlar aracılığıyla yapılması etik olmayan riskli davranışlara odaklanıldığı görülmektedir. Bu nedenle Faktör 4, "Başkalarına Zarar Verme Riskleri" olarak isimlendirilmiştir. Geliştirilen aday ÇRAE ölçeği formu yorumlanabilir yapıdadır. Aynı zamanda kuramsal yapıyla da oldukça uyumludur.

2.5.6. Aday ÇRAE ölçeği DFA aşaması katılımcıları

Aday ÇRAE ölçeğinin DFA aşaması için hedef evreni temsil etmesi ve araştırma verilerinin toplandığı aşamalarda aynı öğrencilerden veri toplamayı engellemek amacıyla araştırma evreni ve katılımcıları başlığında belirtilen Tablo 2.1'de yer alan Eskişehir Osmangazi Üniversitesi'nde, 2000'in üzerinde öğrenci sayısına sahip, dört farklı fakülteden veri toplanmıştır. Mühendislik Fakültesi, Fen Edebiyat Fakültesi, İktisadi ve İdari Bilimler Fakültesi ve Eğitim Fakültesi'nde öğrenim gören 1193 katılımcıdan veri toplanmıştır. Elde edilen veriler incelenmiş ve ilgili ölçeğe hepsini aynı puan (hepsi 5, hepsi 1 vb.) girmiş, desen oluşturarak işaretleme yapmış ve maddelerin yarısından fazlasını boş bırakmış 254 katılımcının verileri DFA aşamasında değerlendirmeye alınmamıştır. Bu doğrultuda aday ÇRAE ölçeğinin DFA çalışmaları için 939 katılımcıya ait veriler kullanılmıştır. Bu aşamadaki veriler AFA aşamasında kullanılan verilerden farklıdır. Çünkü ölçek geliştirmenin AFA sürecinde değişkenlerin birbirleri arasındaki

ilişkiler dikkate alınmaktadır (Wothington ve Wihittaker, 2006), DFA aşamasında ise AFA sonucunda faktörel olarak ulaşılan ölçek yapısının söz konusu örneklemde test edilmesi amaçlanmaktadır. Yani değişkenler arasında AFA sonucu ortaya çıkmış olan ilişkilerin doğrulanıp doğrulanmadığına bakılır. Ölçek geliştirme süreci DFA aşamasında kullanılan örneklem büyüklüğü için aday ölçekteki madde sayısı temel alınabilir. Wothington ve Wihittaker (2006) her madde için minimum beş, ideal olarak ise her madde için on katılımcı sayısına ulaşılmasını önermektedir. Kline (2012) ise 100 ile 200 arasındaki katılımcı sayısına ulaşılmasını önermiştir. Bu anlamda analize tabi tutulan 939 katılımcıdan edinilen veri seti DFA için uygun büyüklüktedir ve bu katılımcılara ilişkin ayrıntılı bilgi ve özellikler Tablo 2.19'da görülmektedir.

Tablo 2.19. *Aday ÇRAE ölçeğinin DFA aşaması katılımcı bilgileri*

		Kadın	Kadın %	Erkek	Erkek %	Toplam	Toplam %
Yaş Aralığı		17-35	-	18-44	-	-	-
Fakülte	Fen Edebiyat Fakültesi	86	20	56	11,2	142	15,1
	Eğitim Fakültesi	161	37,4	76	15,1	237	25,2
	İktisadi ve İdari Bilimler Fakültesi	129	29,9	124	24,7	253	26,9
	Mühendislik Fakültesi	55	12,8	246	49	301	32,1
Toplam		431	100	502	100	939	100
Sınıf	1. sınıf	172	40,1	174	34,7	346	36,8
Düzeyi	2. sınıf	86	20	90	18	176	18,7
	3. sınıf	91	21,2	104	20,8	195	20,8
	4. sınıf	64	14,9	103	20,6	167	17,8
	Hazırlık	2	0,5	-	-	2	0,2
	Diğer	14	3,3	30	6	44	4,7
Toplam		429	100	501	100	939	100
İnternet	0-1 yıl	3	0,7	-	-	3	0,3
Kullanım	2-3 yıl	9	2,1	4	0,8	13	1,4
Durumu	4-5 yıl	60	14	43	8,6	103	11
	6-7 yıl	129	30,1	100	20,1	228	24,3
	8 yıl ve üstü	228	53,3	351	70,5	579	61,7
Toplam		428	100	498	100	939	100
İnternet	Haftada 0-2 saat	4	0,9	4	0,8	8	0,9
Kullanım	Haftada 2-5 saat	11	2,6	13	2,6	24	2,6
Sıklığı	Günde 0-2 saat	47	10,9	74	14,8	121	12,9
	Günde 3-5 saat	207	48,1	226	45,2	433	46,1
	Günde 5-7 saat	150	34,9	163	32,6	313	33,3
	Diğer	11	2,6	20	4	31	3,3
Toplam		430	100	500	100	939	100

Aday ÇRAE ölçeğinin DFA aşamasında analize tabi tutulan 939 katılımcının 431 (%45,9)'i kadın, 504 (%53,7)'ü erkek üniversite öğrencilerinden oluşmaktadır. Katılımcılardan 4 (%0,4)'ü ise cinsiyet bilgisini belirtmemiştir. Tablo 2.19'da belirtildiği

gibi aday ÇRAE ölçeğinin DFA aşaması için yanıt veren kadın katılımcıların yaş aralıkları 17-35, erkek katılımcıların ise 18-44'tür. Katılımcıların öğrenim gördükleri fakülteler incelendiğinde en fazla kadın katılımcının (%37,4) Eğitim Fakültesi, en az kadın katılımcının (%12,8) ise Mühendislik Fakültesi'nde öğrenim gördüğü, erkek katılımcıların ise en fazla Mühendislik Fakültesi (%49), en az erkek katılımcının (%11,2) ise Fen Edebiyat Fakültesi'nde öğrenim gördüğü görülmektedir. Sınıf düzeyi bakımından incelendiğinde en fazla katılımcının (%36,8) 1. sınıf, onu takiben de en fazla katılımcının (%20,8) 3. sınıf düzeyinde olduğu görülmektedir. Katılımcıların internet kullanım durumları incelendiğinde en fazla katılımcının (%61,7) 8 yıl ve üstü süredir internet kullanıcısı olduğu, sadece üç katılımcının ise bir yıldır internet kullanıcısı olduğu dikkat çekmektedir. İnternet kullanım sıklığı açısından bakıldığında en fazla katılımcının (%46,1) günde 3-5 saat aralığında İnternet kullandığı, onu takip eden en fazla katılımcının (%33,3) ise günde 5-7 saat aralığında İnternet kullandığı görülmektedir.

2.5.7. Aday ÇRAE ölçeği DFA süreci

Doğrulayıcı faktör analizi (DFA) daha önceden oluşturulmuş bir modelin, doğrulanıp, doğrulanmadığını sınayan bir analizdir (Çokluk, Şekercioğlu ve Büyüköztürk, 2012). AFA sonuçlarına göre elde edilen modelin, yapı geçerliğini değerlendirmek amacıyla DFA'ya başvurulmuştur (Kline, 2015). Aday ÇRAE ölçeği AFA sonucunda 19 maddeli (Ek 6) dört faktörlü yapıya ulaşılmıştır. Aday ÇRAE ölçeğinin DFA aşaması için Eskişehir Osmangazi Üniversitesi 2000 üstü öğrenci sayısına sahip dört farklı fakülteden veri toplanmış, DFA'da 939 kişilik veri seti analiz edilmiştir.

Bu çalışmada 19 gözlenen değişken ile dört gizil değişkene ilişkin bir ölçme modeli oluşturulmuştur. Model uyumu değerlendirilirken kritik indeksler olarak Tablo 2.20'de belirtilen; $\chi 2$/sd (ki-kare/serbestlik derecesi), yaklaşık hataların ortalama karekökü (RMSEA), standardize edilmiş ortalama hataların karekökü (SRMR), normlaştırılmış uyum indeksi (NFI), normlaştırılmamış uyum indeksi (NNFI) ve karşılaştırmalı uyum indeksi (CFI) göz önünde bulundurulmuştur. Dört faktörlü ölçme modeli için 939 kişilik veri seti ile gerçekleştirilen DFA sonucunda ulaşılan uyum iyiliği indeksleri Tablo 2.21'de sunulmuştur. Model uyumu değerlendirilirken çıkarımsal değerlendirme için $\chi 2$ testi, betimsel değerlendirmeler için ise genel uyum ölçütleri, model karşılaştırmalarına dayalı ölçütler ve model benzetimi ile ilgili ölçütler kullanılmaktadır (Schumacker ve Lomax, 1996, s. 119).

Tablo 2.20. *Model Uyum İndeksleri*

Uyum İndeksi	İyi Uyum Değeri	Kabul Edilebilir Uyum Değeri	Kaynak
χ^2	$0 \leq \chi^2 \leq 2sd$	$2sd < \chi^2 \leq 3sd$	(Tabachnick ve Fidell, 2012; Sütütemiz, 2005)
p değeri	$.05 \leq p \leq 1.00$	$.01 \leq p \leq .05$	(Hoyle, 1995)
χ^2/sd	$0 \leq \chi^2/sd \leq 2$	$2 \leq \chi^2/sd \leq 3$	(Schermelleh-Engel, Moosbrugger ve Müller, 2003)
		$2 \leq \chi^2/sd \leq 5$	(Wheaton, Muthen, Alwin, ve Summers, 1977, s. 99; Marsh ve Hocevar, 1985, s. 576; Kelloway, 1998 (Akt. Erkorkmaz, Etikan, Demir, Özdamar ve Sanisoğlu, 2013))
RMSEA	$0 \leq RMSEA \leq .05$	$.05 \leq RMSEA \leq .08$	(Browne ve Cudeck, 1992; Hu ve Bentler, 1999, s. 27; Schreiber, Nora, Stage, Barlow ve King, 2006)
SRMR	$0 \leq SRMR \leq .05$	$.05 \leq SRMR \leq .10$	(Hu ve Bentler, 1999, s. 27)
NFI	$.95 \leq NFI \leq 1.00$	$.90 \leq NFI < .95$	(Schermelleh-Engel, Moosbrugger ve Müller, 2003; Tabachnick ve Fidell, 2012)
NNFI	$.97 \leq NNFI \leq 1.00$	$.95 \leq NNFI < .97$	(Hu ve Bentler, 1999, s. 27)
CFI	$.97 \leq CFI \leq 1.00$	$.95 \leq CFI < .97$	(Hu ve Bentler, 1999, s. 27; Tabachnick ve Fidell, 2012)

χ^2; sd;

DFA sonucunda çıkarımsal olarak anlamsız sonuç vermesi gereken χ2 testi büyük örnekleme sahip çalışmalarda anlamlı çıktığı görülmektedir. Bunun nedeninin ise hesaplanan χ2 değerinin örneklem sayısından oldukça fazla etkilendiği ve kovaryans matrislerinde tahmin edilen ve gözlenen değerler arasındaki önemsiz farkların anlamlı çıkması olarak belirtilmektedir (Çelik ve Yılmaz, 2013; Fan, Thompson ve Wang, 1999; Floyd ve Wideman, 1995; Lomax ve Schumacker, 2010, s. 86; Ullman ve Bentler, 2012, s. 671; Wheaton, Muthen, Alwin ve Summers, 1977, s. 99). Bu durumda da Tablo 2.21'de görülen ve istatistiksel açıdan anlamlı olan p değeri (<.001) dikkate alınmadan model uyumu değerlendirilmiştir. Serbestlik derecesi (sd)'nin χ2 testinde önemli bir ölçüt olması, uyum ölçütlerinde χ2/sd oranının değerlendirilmesinin uygun bir uyum belirtisi olarak kabul edilmesine sebep olmaktadır (Kelloway, 1998 (Akt. Erkorkmaz vd., 2013); Schermelleh-Engel, Moosbrugger ve Müller, 2003; Wheaton, Muthen, Alwin ve Summers, 1977, s. 99). Bunun yanında Lomax ve Schumacker, (2010, s. 91) model uyum iyiliği indeksleri değerlendirilirken χ2, RMSEA, SRMR indekslerinin her durumda rapor edilmesi gerektiğini belirtmiştir. Bu doğrultuda Tablo 2.21'de χ2 değerine de yer verilmiştir. Ölçme modeline ilişkin Tablo 2.21'deki uyum indeksleri incelendiğinde değerlerin genel olarak kabul edilebilir değerler aralığında olduğu görülmektedir. Schermelleh-Engel, Moosbrugger ve Müller (2003), modelde gözlenen χ2/sd değerinin 3

ve 3'ün altında olması, modelin kabul edilebilir bir uyum göstergesine sahip olduğunun bir göstergesi olduğunu belirtmiştir.

Tablo 2.21. *Aday CRAE ölçeğinin 939 kişilik veri seti ile yapılan DFA sonucunda elde edilen uyum değerleri*

Uyum İndeksi	İyi Uyum Değeri	Kabul Edilebilir Uyum Değeri	Gözlenen Uyum Değeri	Değerlendirme
χ^2	$0 \leq \chi^2 \leq 2sd$	$2sd \leq \chi^2 \leq 3sd$	394.26<438	-
p değeri	.05≤p≤1.00	.01 ≤p≤ .05	.000	-
χ^2/sd	0≤ /sd≤2	$2 \leq \chi^2/sd \leq 3$	2.7	Kabul edilebilir uyum
RMSEA	0≤RMSEA≤.05	.05≤RMSEA≤.08	.043	İyi uyum
SRMR	0≤SRMR≤.05	.05≤SRMR≤.10	.04	İyi uyum
NFI	.95≤NFI≤1.00	.90≤NFI<.95	.944	Kabul edilebilir uyum
NNFI	.97≤NNFI≤1.00	.95≤NNFI<.97	.958	Kabul edilebilir uyum
CFI	.97≤CFI≤1.00	.95≤CFI<.97	.964	Kabul edilebilir uyum
χ^2=394.26; sd=146				

Tablo 2.21'e bakıldığında, belirtilen χ2/sd=2,7 değeri, kabul edilebilir bir uyum değeri olarak ele alınabilir. Hu ve Bentler (1999, s. 27) ve Browne ve Cudeck (1992, s. 239), RMSEA uyum indeksinin <.05 olmasını iyi uyum, <.08 olmasını ise değerlendirilebilir yani kabul edilebilir uyum olduğunu belirtmektedirler. Bu doğrultuda aday ölçeğin sahip olduğu .043 RMSEA değeri iyi uyum değeri olarak yorumlanabilir. SRMR uyum indeksinin <.05 olması iyi uyum değeri (Lomax ve Schumacker, 2010, S. 91), <.10 olması ise kabul edilebilir uyum değeri olarak yorumlanmaktadır (Hu ve Bentler, 1999 s. 27). Dolayısıyla aday ölçeğin SRMR uyum değerinin .04 olması, iyi uyum değerine sahip olduğunu göstermektedir. Schermelleh-Engel, Moosbrugger ve Müller (2003) ve Tabachnick ve Fidell (2012)'e göre NFI uyum indeksinin .95 ile 1.00 aralığında olması iyi uyum değeri, .90 ile .95 aralığında olması ise kabul edilebilir uyum değeri olarak yorumlanmaktadır. Bu doğrultuda aday ölçeğin sahip olduğu NFI uyum indeksinin .944 olması kabul edilebilir uyuma sahip olduğunun bir göstergesi olarak söylenebilir. NNFI ve CFI uyum indekslerinin değerleri .97 ve 1.00 aralığında iyi uyum, .95 ile .97 aralığında ise kabul edilebilir uyum değeri olarak yorumlanmaktadır (Hu ve Bentler, 1999, s. 27; Tabachnick ve Fidell, 2012). Aday ölçeğin NNFI uyum indeks değeri .958 ve CFI uyum indeks değerinin .964 olması kabul edilebilir uyum değerlerine sahip olduğunun bir göstergesi olarak kabul edilebilir. Özetle aday ölçeğin 939 kişilik veri seti ile gerçekleştirilmiş DFA sonucuna göre, χ2/sd, NFI, NNFI ve CFI değerlerinin

"kabul edilebilir uyum", RMSEA, SRMR değerlerinin ise "iyi uyum" değer aralıklarında olduğu görülmektedir.

Floyd ve Wideman (1995, s. 245), örneklem büyüklüğüne duyarlı olan ki-kare değeri sorununu aşmak için örneklemi küçük alt bölümlere ayırıp, DFA'nın tekrarlanmasını ve ek kanıt elde edilmesini önermiştir. Bu doğrultuda 939 kişilik örneklem büyüklüğüne sahip veri setinden rastgele 300, 400 ve 500 kişilik veri setleri oluşturulmuş ve bu veri setleriyle DFA tekrarlanmıştır. İlgili örneklem büyüklüklerine ait DFA değerleri Tablo 2.22'de sunulmuştur.

Tablo 2.22. *DFA aşamasında toplanan veri setinden rastgele seçim ile oluşturulan örneklemlerin analizi sonucunda elde edilen uyum değerleri*

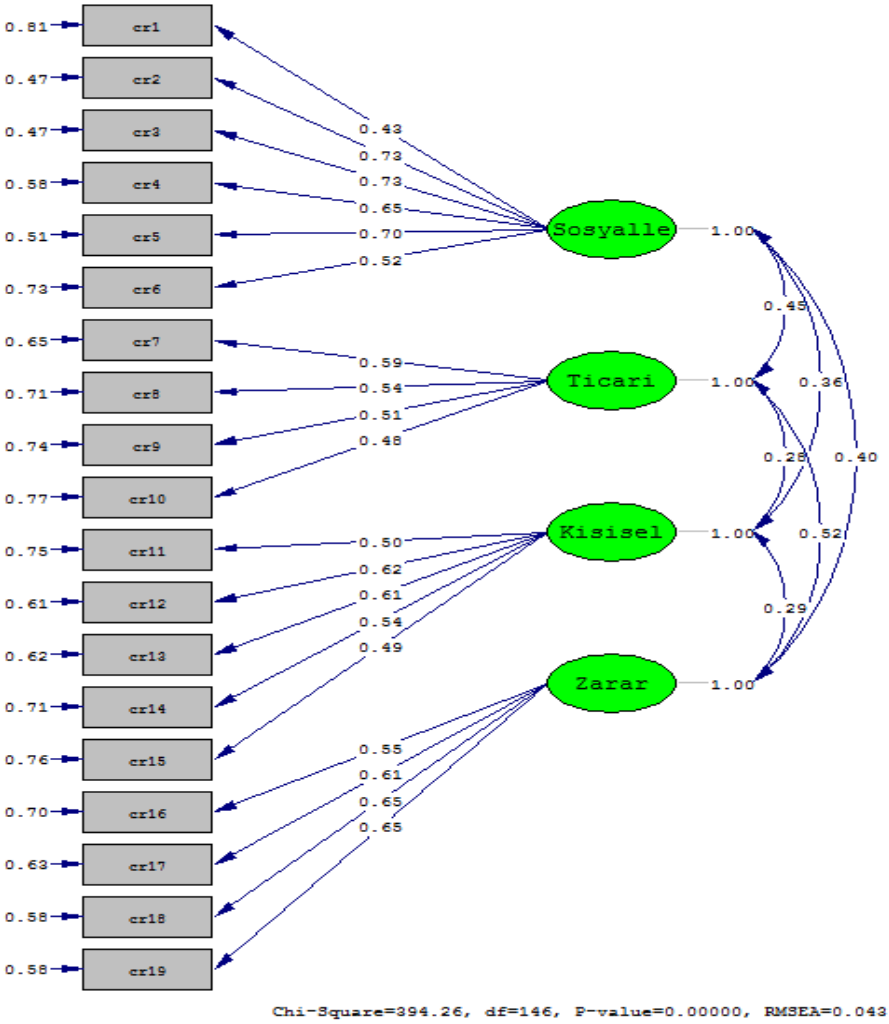
Uyum İndeksi	İyi Uyum	Kabul Edilebilir Uyum	Örneklem Büyüklüğü (n)	Gözlenen Değer
χ^2	$0 \leq \chi^2 \leq 2sd$	$2sd \leq \chi^2 \leq 3sd$	300	218.67<2sd
			300	229.06<2sd
			400	256.06<2sd
			400	261.77<2sd
			500	272.04<2sd
			500	326.15<3sd
p değeri	.05 <p ≤ 1.00	.01 ≤ p ≤ .05	300	.000
			300	.000
			400	.000
			400	.000
			500	.000
			500	.000
χ^2/sd	$0 \leq \chi^2/sd \leq 2$	$2 \leq \chi^2/sd \leq 3$	300	1.49
			300	1.56
			400	1.75
			400	1.79
			500	1.86
			500	2.23
RMSEA	0 ≤ RMSEA ≤ .05	.05 <RMSEA ≤ .08	300	.041
			300	.044
			400	.042
			400	.045
			500	.042
			500	.050
SRMR	0 ≤ SRMR ≤ .05	.05 <SRMR ≤ .10	300	.054
			300	.061
			400	.052
			400	.050
			500	.047
			500	.049
NFI	.95 ≤ NFI ≤ 1.00	.90 ≤ NFI <.95	300	.905
			300	.905
			400	.920
			400	.921

Tablo 2.22. (Devam) *DFA aşamasında toplanan veri setinden rastgele seçim ile oluşturulan örneklemlerin analizi sonucunda elde edilen uyum değerleri*

Uyum İndeksi	İyi Uyum	Kabul Edilebilir Uyum	Örneklem Büyüklüğü (n)	Gözlenen Değer
NFI	.95 ≤ NFI ≤ 1.00	.90 ≤ NFI <.95	500	.929
			500	.929
NNFI	.97 ≤ NNFI ≤ 1.00	.95 ≤ NNFI <.97	300	.960
			300	.956
			400	.957
			400	.957
			500	.959
			500	.952
CFI	.97 ≤ CFI ≤ 1.00	.95 ≤ CFI <.97	300	.966
			300	.963
			400	.964
			400	.963
			500	.965
			500	.959
sd: 146				

939 kişilik veri setinden rastgele seçilmiş 300, 400 ve 500 kişilik örneklemlerle denenmiş DFA'ları sonuçları Tablo 2.22'de sunulmuştur. Bu tablodaki uyum değerleri incelendiğinde örneklem sayısı (n) küçüldükçe $\chi 2$ değerinin azaldığı ve $\chi 2/sd$'nin iyi uyum değerine sahip olduğu görülmektedir. DFA'da genellikle, $\chi 2$ ve $\chi 2/sd$ ($0 \leq \chi 2/sd \leq 2$) değerlerinin "İyi uyum" aralığında değer aldığı görülmektedir (Schermelleh-Engel, Moosbrugger ve Müller, 2003; Sütütemiz, 2005; Tabachnick ve Fidell, 2012). RMSEA değerinin "İyi uyum", SRMR değerlerinin genellikle "Kabul edilebilir uyum" (Browne ve Cudeck, 1992; Hu ve Bentler, 1999, s. 27), CFI, NFI ve NNFI değerlerinin ise "Kabul edilebilir uyum" (Hu ve Bentler, 1999, s. 27; Tabachnick ve Fidell, 2012) değer aralıklarında olduğu görülmektedir. Bu doğrultuda aday ölçeğin Tablo 2.21 ve Tablo 2.22'deki uyum indeks değerleri incelendiğinde oluşturulan ölçme modelinin doğrulandığı ifade edilebilir.

Aday ölçeğin DFA'sına ilişkin her maddesine ait standardize çözümleme değerlerinin anlamlı olup olmadığını değerlendirmek için t değerleri incelenmiş ve bu değerlerin 12.47 ile 23.85 arasında değiştiği görülmüştür. Tüm maddeler için hesaplanan t değerleri $p<.01$ düzeyinde anlamlı bulunmuştur. Aday ölçeğin DFA sonrası elde edilen uyum indeks değerleri doğrultusunda, 19 maddelik ölçme aracının kabul edilebilir bir uyum gösterdiği aynı zamanda uygulanabilir olduğu görülmüştür. Şekil 2.7'de çevrimiçi risk alma eğilimi aday ölçeğinin dört faktörlü yapısına ilişkin düzenlenen yol diyagramı sunulmuştur.



Şekil 2.3. *Çevrimiçi Risk Alma Eğilimi aday ölçeği DFA'ne ilişkin düzenlenen yol diyagramı (Standartlaştırılmış Değerler)*

Çevrimiçi Risk Alma Eğilimi (ÇRAE) ölçeğinin ölçmeye yöneldiği yapıyı ölçüp ölçmediğine ilişkin yapı geçerliği; yakınsama geçerliği (convergent validity) ve ıraksama geçerliğinin (divergent validity) bir diğer versiyonu olan ayırt edici geçerlilik (diskriminant validity) teknikleri kullanılarak incelenmiştir. Yapı güvenirliği ve Cronbach Alfa katsayısı kullanılarak ölçme aracından elde edilen verilerin içtutarlılık anlamındaki güvenirliği irdelenmiştir. Nunnally ve Bernstein (1994)'a göre ölçme sonuçlarının güvenirliğine ilişkin bir kanıt olarak, ölçeğin her bir boyutuna ilişkin alfa katsayılarının ve yapısal güvenirlik değerlerinin 0.70'ten büyük olması gerektiği belirtilmektedir. Tablo 2.23 incelendiğinde ölçek boyutlarına ilişkin yapısal güvenirlik değerlerinin .70'ten büyük olduğu görülmektedir. Fakat bu ölçeğin alt boyutlarına ait alfa güvenirlik katsayıları incelendiğinde bir alt boyutun alfa güvenirlik katsayısı .60, diğer

boyutlara ait alfa güvenirlik katsayılarının ise .70 ve üstü olduğu görülmektedir. Geliştirilen ÇRAE ölçeğinin geçerlik ve güvenirlik analiz sonuçları Tablo 2.23' te belirtilmiştir.

Tablo 2.23. *ÇRAE ölçeği DFA özeti*

Değişkenler	Ortalama	ss	Faktör Ortalamaları	ss	Alpha Güvenirliği	Yapısal Güvenirlik	Ortalama Açıklanan Varyans	Madde Yükü	t değeri	Hata
Sosyalleşme Riskleri										
CR1	1.91	.882	2.076	.723	.80	.84	.47	.532	12.72	0.63
CR2	2.12	1.061						.786	23.69	0.53
CR3	2.08	1.032						.761	23.85	0.50
CR4	1.65	.986						.678	20.41	0.56
CR5	2.40	1.123						.724	22.63	0.64
CR6	2.30	1.046						.603	15.79	0.79
Ticari Riskler										
CR7	1.74	1.171	1.991	.822	.60	.74	.41	.654	15.29	0.90
CR8	1.71	1.162						.662	14.01	0.96
CR9	2.01	1.150						.622	13.14	0.98
CR10	2.51	1.402						.633	12.47	1.51
Kişisel Bilgileri Açma Riskleri										
CR11	2.46	1.168	2.367	.777	.70	.79	.43	.561	13.71	1.02
CR12	2.20	1.151						.689	17.25	0.81
CR13	2.18	1.148						.728	17.04	0.82
CR14	2.53	1.165						.681	14.82	0.96
CR15	2.46	1.176						.597	13.35	1.05
Başkalarına Zarar Verme Riskleri										
CR16	1.33	.694	1.304	.476	.70	.80	.51	.694	15.54	0.34
CR17	1.33	.654						.729	17.30	0.27
CR18	1.20	.524						.731	18.67	0.16
CR19	1.36	.719						.693	18.73	0.30
n: 939; açıklanan varyans: %49.594										

George ve Mallery (2003, s. 231)'e göre alfa güvenirlik katsayısının .50'den küçük olmasının kabul edilemeyecek güvenirlik katsayısı olduğunu belirtmiştir. Aynı zamanda Hair Jr, Hult, Ringle ve Sarstedt (2017, s.136)'de yeni geliştirilen ölçme araçlarında alfa güvenirlik katsayısının .60 ile .70 aralığında olmasının kabul edilebilecek bir değer olduğu, aksi taktirde bu katsayının .70 ile .90 değerleri arasında olmasının istenen

değerler olduğu belirtilmektedir. Bu doğrultuda ilgili ölçeğin güvenilir olduğu ifade edilebilir.

Yakınsak geçerlilik için çeşitli yollar mevcuttur. Bu yollar arasında faktör yüklerinin, Ortalama Açıklanan Varyans (OAV) değerlerinin ve yapısal güvenirlik değerlerinin incelenmesi yer almaktadır. Madde Faktör yüklerinin .5 veya daha yüksek bir değere sahip olması özellikle .7 ve üstü bir değerin yakınsak geçerlik için daha ideal bir değer olduğu belirtilmektedir (Hair, Black, Babin ve Anderson, 2009, s. 679). Bu durumda öncelikle faktörleri oluşturan maddelerin faktör yükleri incelenmiş ve her bir boyuta ilişkin maddelerin faktör yüklerinin .532 ile .786 arasında değişen değerler aldıkları görülmüştür. Fornell ve Larcker (1981, s. 46) yakınsak geçerlik için OAV değerlerinin .5 ve üstü olması gerektiğini belirtmektedir. Fakat söz konusu ölçeğin boyutlarına ait OAV değerlerinin .41 ile .51 aralığında olduğu görülmektedir. Hair vd. (2009, s. 680) ölçek boyutlarının yapısal geçerlik değerlerinin .7 ve üstü olması iyi güvenirliği gösterirken, bir modelin yapı geçerliliğinin diğer göstergelerinin iyi olması koşuluyla .6 ile .7 arasındaki güvenirlik değerlerinin de kabul edilebileceği belirtilmiştir. Tablo 2.23'te görüldüğü üzere ölçek boyutlarına ilişkin yapısal güvenirlik değerlerinin .74 ile .84 aralığında olduğu görülmektedir. Bu doğrultuda faktör yükleri ve yapısal güvenirlik değerleri söz konusu ölçeğin yakınsama geçerliğinin bir kanıtı olarak gösterilebilir. Ayırt edici geçerlilik için ilgili ölçeğin alt boyutları arasındaki korelasyon ve OAV değerlerinin karekökünden yararlanılmaktadır.

Ayırt edici geçerliliğin sağlanması için ölçeğin her bir alt boyutlara ilişkin OAV değerlerinin kareköklerinin, o alt boyutun diğer alt boyutlar ile aralarındaki korelasyondan ve aynı zamanda 0.50 değerinden küçük olmaması gerekmektedir (Fornel ve Larcker, 1981, s. 46). ÇRAE ölçeği faktörleri arasındaki korelasyonlar ve OAV değeri kareköklerı Tablo 2.24'te sunulmuştur.

Tablo 2.24. *ÇRAE ölçeği faktörleri arasındaki korelasyon ve OAV değeri karekökü*

Boyutlar	**Sembol**	**Ortalama**	**Ss**	**[1]**	**[2]**	**[3]**	**[4]**
Sosyalleşme Riskleri	[1]	2.07	0.72	**0.68**			
Ticari Riskler	[2]	1.99	0.82	.313**	**0.64**		
Kişisel Bilgileri Açma Riskleri	[3]	2.36	0.77	.307**	.216**	**0.65**	
Başkalarına Zarar Verme Riskleri	[4]	1.30	0.47	.307**	.316**	.198**	**0.71**

** 0.01 düzeyinde anlamlıdır.

Tablo 2.24 incelendiğinde, ölçeğin her alt boyutunun OAV değerlerinin karekökleri, boyutlar arasındaki korelasyon değerinden ve 0.50 değerinden daha büyüktür. Örneğin, Sosyalleşme Riskleri alt boyutunun OAV karekökü değeri 0.68'dir. Söz konusu alt boyutun OAV değeri diğer alt boyutlar ile olan korelasyonundan daha büyüktür. Bu doğrultuda ölçeğin ayırt edicilik geçerliğinin sağlandığı söylenebilir.

2.6. Veri Analizi

Araştırma verileri Anadolu Üniversitesi dört yıllık fakültelerinde farklı fakülte ve bölümlerde öğrenim görmekte olan 1729 üniversite öğrencisinden toplanmıştır. Veri seti hatalı veri girişi ihtimaline ilişkin incelenmiş ve daha sonra kayıp veri analizine tabi tutulmuştur. Kullanılan ölçme araçlarının maddelerine %0-%2,3 oranları aralığında yanıt verilmediği görülmüştür. Dolayısıyla kayıp veriler maddelere verilen yanıtların ortalamaları ile doldurulmuştur. Daha sonra yapılacak çıkarımsal istatistiklerin varsayımlarını test etmek amacıyla veri setindeki uç değerler, ölçeklerin faktörleri ortalamalarının z puanları hesaplanarak incelenmiştir. Z puanları |3,33| değeri üzerindeki değerler veri setinden çıkartılmıştır. Araştırma soruları çerçevesinde kullanılan veri toplama araçları ve veri analizi teknikleri Tablo 2.25'te görüldüğü gibidir.

Tablo 2.25. *Veri analiz süreci*

Araştırma Soruları	Veri Toplama Aracı	Veri Analizi
1. Üniversite öğrencilerinin dijital güvenlik öz yeterlikleri, şimdiki çevrimiçi risk alma eğilimleri ve geçmişteki çevrimiçi risk alma eğilimleri • Cinsiyete, • Yaş gruplarına, • Öğrenim gördükleri bilim dallarına, • İnternet kullanım sıklıklarına göre istatistiksel olarak farklılaşmakta mıdır?	Demografik bilgi formu Dijital Güvenlik Öz Yeterlik Ölçeği (DGÖY) Çevrimiçi Risk Alma Eğilimi Ölçeği (ÇRAE)	Betimsel İstatistikler (%, f, x, ss) Bağımsız Örneklemler t Testi Tek Yönlü Varyans Analizi (ANOVA)
2. Üniversite öğrencilerinin dijital güvenlik öz yeterlikleri, şimdiki çevrimiçi risk alma eğilimleri ve geçmişteki çevrimiçi risk alma eğilimleri arasındaki ilişkiler nasıldır?		Korelasyon
3. Üniversite öğrencilerinin geçmişteki çevrimiçi risk alma eğilimleri, şimdiki çevrimiçi risk alma eğilimlerini yordamakta mıdır?		Çoklu Doğrusal Regresyon

Çoklu normal dağılımı sağlamak amacıyla ölçek faktörleri puanlarının Mahalanobis uzaklıkları incelenmiş ve burada veri setinde yer alan uç değerler de veri setinden çıkartılmıştır. Son olarak 1601 katılımcıdan oluşan veri setinin normal dağılımı basıklık ve çarpıklık katsayıları incelenerek belirlenmiştir. Veriler analiz edilmeden önce katılımcıların yaş, öğrenim gördükleri bölüm, sınıf düzeyleri, internet kullanım sıklıkları sürekli değişkenleri üzerinde istatistiksel testler yapılabilmesi için yoğunlaştıkları aralığa göre gruplandırmalar yapılmıştır. Tablo 2.26'da katılımcıların çevrimiçi risk alma eğilimleri ve dijital güvenlik öz yeterliklerinin incelendiği bağımsız değişkenlerin gruplandırmaları yer almaktadır.

Tablo 2.26. *Araştırma verileri analizinde kullanılan değişkenlerin gruplandırılması*

		Kadın	Kadın %	Erkek	Erkek %	Toplam	Toplam %
Yaş	21 yaş ve altı	669	66,7	334	33,3	1003	63,2
	22 yaş ve üstü	297	50,9	287	49,1	584	36,8
Toplam		966	60,9	621	39,1	1587	100
Bilim	Sosyal Bilimler	623	62,4	375	37,6	998	63,3
alanları	Fen Bilimleri	345	59,6	234	40,4	579	36,7
Toplam		968	61,4	609	38,6	1577	100
İnternet	Günde 3 saat ve altı	153	56	120	44	273	17,2
Kullanım	Günde 3-5 saat	468	62,4	282	37,6	750	47,2
Sıklıkları	Günde 5 saat ve üstü	350	61,9	215	38,1	565	35,6
Toplam		971	61,1	617	38,9	1588	100

Tablo 2.26'da katılımcıların yaş bilgilerinin yoğunlaştığı aralıklar 21 yaş ve altı ve 22 yaş ve üstünde olmak ikiye ayrılmıştır. 21 yaş ve altında 1003 (%63,2), 22 yaş ve üstünde ise 584 (%36,8) katılımcı vardır. Araştırma katılımcılarının bölümlerine göre hangi bilim dalına göre öğrenim gördükleri belirlenmiştir. Bu bağlamda katılımcıların 998 (%63,3)'i Sosyal Bilimler, 579 (%36,7)'u Fen Bilimleri bilim dallarına ait bölümlerde öğrenim görmektedirler. İnternet kullanım sıklıklarına bakıldığında ise haftalık internet kullanım aralıklarında ve diğer olarak belirtilip günde 8 saat ve üstü internet kullanım süreleri olan katılımcılardan diğer gruplara oranla daha az sayıda oldukları görülmüştür. Bu durumda verilerin yoğunlaştıkları bu aralıklar günde 3 saat ve altı, günde 3-5 saat arası ve günde 5 saat ve üstü sıklığında internet kullananlar olarak gruplandırılmıştır. Katılımcıların 273 (17,2)'ü Günde 3 saat ve altında, 750 (%47,2)'si

günde 3-5 saat aralığında ve 565 (35,6)'sının ise günde 5 saat ve üstünde internet kullandıkları görülmektedir.

3. BULGULAR VE YORUM

Bu bölümde, araştırmanın genel amacı ve alt amaçları doğrultusunda gerçekleştirilen betimsel, çıkarımsal istatistiksel analizler sonucu elde edilen bulgular ve yorumlarına yer verilmiştir.

3.1. Üniversite Öğrencilerinin Dijital Güvenlik Öz Yeterlik Düzeyleri, Şimdiki ve Geçmişteki Çevrimiçi Risk Alma Eğilimlerine İlişkin Betimsel Bulgular

Tablo 3.1, Tablo 3.2 ve Tablo 3.3'te, kullanılan veri toplama araçlarının toplamda ve ilgili ölçeklerin boyutları çerçevesinde çarpıklık ve basıklık katsayıları görülmektedir. Tablo 3.1'de üniversite öğrencilerinin dijital güvenlik öz yeterlik ölçeği normallik dağılımı ve bu ölçeğin faktörlerine ilişkin ortalamalar sunulmuştur.

Tablo 3.1. *Dijital güvenlik öz yeterlik ölçeği normallik dağılımı*

Dijital Güvenlik Öz Yeterlik Ölçeği Boyutları	**n**	**Min.**	**Maks.**	**x̄**	**ss**	**Ç**	**B**
Dijital Uygulamalarda Güvenlik	1601	2,82	5,00	4,561	,479	-1,091	,500
Dijital Araçlarda Güvenlik	1601	1,33	5,00	3,886	,798	-,438	-,413
Toplam	1601	2,26	5,00	4,209	,580	-,484	-,461

Tablo 3.1 incelendiğinde dijital güvenlik öz yeterlik ölçeğinin geneli ve alt boyutlarının çarpıklık katsayılarının |-1,091| ile |-,438|, basıklık katsayılarının ise |,500| ile |-413| aralıklarında yer aldığı görülmektedir. Bu durum Kline (2015)'e göre verilerin normal dağılıma sahip olduğu göstermektedir. Dijital güvenlik öz yeterlik ölçeğinin alt boyutları olan dijital uygulamalarda güvenlik becerileri ortalama puanı x̄= 4,56 ve dijital araçlarda güvenlik becerileri ortalama puanları ise x̄= 3,88'dir. Her iki alt boyuta ilişkin üniversite öğrencilerinin dijital uygulamalarda güvenlik öz yeterlik düzeylerinin dijital araçlarda güvenlik öz yeterliklerinden daha yüksek olduğu söylenebilir. Tablo 4.2'de üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimi ölçeği verilerinin normallik dağılımı ve bu ölçeğin faktörlerine ilişkin ortalamaları sunulmuştur. Üniversite öğrencilerinin şimdiki çevrimiçi risk alma ölçeğinin genelinin ve alt boyutlarının çarpıklık katsayıları |2,020| ile |,471| aralığında, basıklık katsayıları ise |-3,512| ve |-,054| aralığında yer almaktadır. Bu durum Kline (2015)'e göre verilerin normal dağılıma sahip olduğunu göstermektedir.

Tablo 3.2. *Çevrimiçi risk alma eğilimi ölçeği normallik dağılımı (şimdiki)*

Çevrimiçi Risk Alma Ölçeği Alt Boyutları	n	Min.	Max.	x̄	ss	Ç	B
Sosyalleşme Riskleri	1601	1,00	4,67	1,942	,721	,803	,326
Ticari Riskler	1601	1,00	5,00	1,873	,818	1,006	,607
Kişisel Bilgileri Açma Riskleri	1601	1,00	5,00	2,283	,857	,471	-,412
Başkalarına Zarar Verme Riskleri	1601	1,00	3,00	1,282	,484	2,020	3,512
Toplam	1601	1,00	3,74	1,878	,535	,635	-,054

Tablo 3.2 incelendiğinde üniversite öğrencilerinin şimdiki çevrimiçi risk alma ölçeğinin genelinin ve alt boyutlarının çarpıklık katsayıları |2,020| ile |,471| aralığında, basıklık katsayıları ise |-3,512| ve |-,054| aralığında yer almaktadır. Bu durum Kline (2015)'e göre verilerin normal dağılıma sahip olduğunu göstermektedir. Üniversite öğrencilerinin içinde bulundukları zamandaki çevrimiçi risk alma eğilimi ölçeğinin alt boyutları olan sosyalleşme risklerine ilişkin ortalama puanı x̄ = 1,94, ticari risklere ilişkin ortalama puanı x̄=1,87, kişisel bilgileri açma riski ortalama puanı x̄=2,28 ve başkasına zarar verme riskine ilişkin olarak ortalama puan ise x̄=1,87'dir. Üniversite öğrencilerinin kişisel bilgileri açma risklerini arasıra, sosyalleşme riskleri, ticari riskler ve başkalarına zarar verme riskleri nadir sıklıkta gösterdiklerini belirtmişlerdir. İlgili boyutlara bakıldığında üniversite öğrencilerinin kişisel bilgilerini açma ve sosyalleşme riskleri boyutlarında, ticari riskler ve başkalarına zarar verme risklerinden daha fazla riskli davranış eğilimi gösterdikleri söylenebilir. Tablo 3.3'te üniversite öğrencilerinin geçmişteki çevrimiçi risk alma eğilimi ölçeği verilerinin normallik dağılımı ve bu ölçeğin faktörlerine ilşkin ortalamaları sunulmuştur.

Tablo 3.3. *Çevrimiçi risk alma eğilimi ölçeği normallik dağılımı (geçmişte)*

Çevrimiçi Risk Alma Ölçeği Alt Boyutları	n	Min.	Maks.	x̄	Ss	Ç	B
Sosyalleşme Riskleri	1601	1,00	5,00	2,188	,821	,485	-,387
Ticari Riskler	1601	1,00	4,75	1,729	,749	1,106	,809
Kişisel Bilgileri Açma Riskleri	1601	1,00	5,00	2,273	,879	,437	-,477
Başkalarına Zarar Verme Riskleri	1601	1,00	3,75	1,409	,587	1,632	2,039
Toplam	1601	1,00	4,05	1,950	,582	,509	-,170

Tablo 3.3 incelendiğinde üniversite öğrencilerinin geçmişte çevrimiçi risk alma eğilimleri genelinin ve alt boyutlarının çarpıklık katsayıları |1,632| ile |,485| aralığında,

basıklık katsayıları ise |2,039| ve |-,170| aralığında yer almaktadır. Bu durum Kline (2015)'e göre verilerin normal dağılıma sahip olduğunu göstermektedir. Çevrimiçi risk alma eğilimi ölçeğinin alt boyutları olan; sosyalleşme risklerine ilişkin ortalama puanı $\bar{x}$= 2,18, ticari risklere ilişkin ortalama puanı $\bar{x}$=1,72, kişisel bilgileri açma riski ortalama puanı $\bar{x}$=2,27 ve başkasına zarar verme riskine ilişkin olarak ortalama puan ise $\bar{x}$=1,40'tır. Üniversite öğrencilerinin sosyalleşme riskleri ve kişisel bilgileri açma risklerini arasıra, ticari riskler ve başkalarına zarar verme risklerini nadir sıklıkta gösterdiklerini belirtmişlerdir. İlgili boyutlara bakıldığında üniversite öğrencilerinin kişisel bilgilerini açma ve sosyalleşme riskleri boyutlarında geçmişe yönelik verilerinde de ticari riskler ve başkalarına zarar verme risklerinden daha fazla riskli davranış eğilimi gösterdikleri söylenebilir. Üniversite öğrencilerinin çevrimiçi risk alma eğilimleri geçmiş ve şimdiki puanlamaları incelendiğinde, geçmişte aldıkları sosyalleşme riskleri, şimdiki sosyalleşme risklerinden daha fazla olduğu söylenebilir.

3.2. Cinsiyete Göre Üniversite Öğrencilerinin Dijital Güvenlik Öz Yeterlik Düzeyleri, Şimdiki ve Geçmişteki Çevrimiçi Risk Alma Eğilimleri

Bu bölümde, üniversite öğrencilerinin, dijital güvenlik öz yeterlik düzeyleri, şimdiki ve geçmişteki çevrimiçi risk alma eğilimlerinin, cinsiyet bağlamında incelenmesi sunulmuştur.

3.2.1. Üniversite öğrencilerinin dijital güvenlik öz yeterlikleri düzeylerinin cinsiyete göre incelenmesi

Üniversite öğrencilerinden elde edilen veriler, birbirinden bağımsız iki grubun sürekli bir değişken üzerinden aldıkları ortalama puanların karşılaştırılmasını sağlayan bağımsız örneklemler için t testi ile analiz edilmiştir. Tablo 3.4'te görüldüğü gibi üniversite öğrencilerinin dijital öz yeterlik düzeylerinin cinsiyetlerine göre farklılaşıp farklılaşmadıkları incelenmiştir. Dijital güvenlik öz yeterlik ölçeğinin dijital uygulamalarda güvenlik boyutu ele alındığında kadın üniversite öğrencilerinin ortalaması ($\bar{x}$=4,543), ile erkek üniversite öğrencilerinin ortalamasının ($\bar{x}$=4,587) olduğu görülmektedir ($t_{(1595)}$=-1,807; p>0,05). Yani dijital güvenlik öz yeterlik ölçeğinin dijital uygulamalarda güvenlik boyutunda kadın üniversite öğrencileri ile erkek üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmamıştır.

Tablo 3.4. *Üniversite öğrencilerinin dijital güvenlik öz yeterlikleri düzeylerinin cinsiyete göre karşılaştırılması*

	Grup	n	x̄	ss	sd	t	p	η2
Dijital uygulamalarda güvenlik	Kadın	975	4,543	,464	1595	-1,807	,071	-
	Erkek	622	4,587	,501				
Dijital araçlarda güvenlik	Kadın	975	3,757	,792	1595	-8,231	,000	0,038
	Erkek	622	4,087	,765				

Tablo 3.4'te görüldüğü üzere, Dijital güvenlik öz yeterlik ölçeğinin dijital araçlarda güvenlik boyutunda ise kadın üniversite öğrencilerinin ortalaması ($\bar{x}$=3,757), erkek üniversite öğrencilerinin ortalamasından ($\bar{x}$= 4,087) daha düşük olduğu görülmektedir ($t_{(1595)}$=-8,231; p<0,001; η^2=0.038). Yani dijital güvenlik öz yeterlik ölçeğinin dijital araçlarda güvenlik boyutunda kadın üniversite öğrencileri ile erkek üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmıştır. Bu istatistiksel farkın kuram ve uygulamadaki önemini etki büyüklükleri göstermektedir ve alanyazında farklı etki büyüklüğü endeksleri ve yorumlamaları bulunmaktadır. η^2 etki büyüklüğü kesme değerleri; .20 için çok büyük, .1379 için büyük, .0588 için orta ve .0099 için kabul edilebilir en düşük etki olarak kabul edilmektedir (Cohen, 1988, s.283; Işık, 2014). Bu doğrultuda dijital araçlarda güvenlik boyutu ile cinsiyetin etki büyüklüğünün (η^2=0.038) küçük düzeyde olduğu söylenebilir. Sonuç olarak üniversite öğrencilerinin dijital uygulamalarda güvenlik öz yeterlik düzeylerinin cinsiyete göre değişmediği, dijital araçlarda güvenlik öz yeterlik düzeylerinin ise erkeklerde kadınlara oranla daha yüksek olduğu belirlenmiştir.

3.2.2. Üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin cinsiyete göre incelenmesi

Bu çalışmayla üniversite öğrencilerinden elde edilen veriler, birbirinden bağımsız iki grubun sürekli bir değişken üzerinden aldıkları ortalama puanların karşılaştırılmasını sağlayan bağımsız örneklemler için t testi ile analiz edilmiştir. Tablo 3.5'te görüldüğü gibi üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimleri cinsiyetlerine göre farklılaşıp farklılaşmadıkları incelenmiştir. Tablo 3.5'te ÇRAE ölçeğinin sosyalleşme riskleri boyutunda kadın üniversite öğrencilerinin ortalaması ($\bar{x}$=1,744), erkek üniversite öğrencilerinin ortalamasından ($\bar{x}$= 2,253) daha düşük olduğu görülmektedir ($t_{(1182,259)}$ =-14,191; p<0,001; η^2=0,112).

Tablo 3.5. *Üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin cinsiyete göre karşılaştırılması*

	Grup	n	x̄	ss	sd	t	p	η2
Sosyalleşme Riskleri	Kadın	975	1,744	,637	1182,259	-14,191	,000	0,112
	Erkek	622	2,254	,737				
Ticari Riskler	Kadın	975	1,537	,589	1003,630	-22,348	,000	0,238
	Erkek	622	2,404	,845				
Kişisel Bilgileri Açma Riskleri	Kadın	975	2,194	,858	1595	-5,217	,000	0,017
	Erkek	622	2,422	,839				
Başkasına Zarar Verme Riskleri	Kadın	975	1,187	,387	980,432	-9,301	,000	0,051
	Erkek	622	1,430	,575				

Tablo 3.5'te görüldüğü üzere, çevrimiçi risk alma eğilimi ölçeğinin sosyalleşme riskleri boyutunda kadın üniversite öğrencileri ile erkek üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmıştır. Bu farkın etki büyüklüğü ise orta düzeydedir. Çevrimiçi risk alma eğilimi ölçeğinin ticari riskler boyutunda, sosyalleşme risklerinde olduğu gibi kadın üniversite öğrencilerinin ortalaması (x̄=1,536), erkek üniversite öğrencilerinin ortalamasından (x̄= 2,403) daha düşük olduğu görülmektedir ($t_{(1003,630)}$ =-22,348; p<0,001; η^2=0.238). Bu durumda, çevrimiçi risk alma eğilimi ölçeğinin ticari riskler boyutunda kadın üniversite öğrencileri ile erkek üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmıştır. Bu farkın etki büyüklüğü çok yüksek düzeydedir. Çevrimiçi risk alma eğilimi ölçeğinin kişisel bilgileri açma riskleri boyutunda kadın üniversite öğrencilerinin ortalaması (x̄=2,194), erkek üniversite öğrencilerinin ortalamasından (x̄= 2,422) daha düşük olduğu görülmektedir ($t_{(1595)}$ =-5,217; p<0,001; η^2=0,017). Bu durumda, çevrimiçi risk alma eğilimi ölçeğinin kişisel bilgileri açma riskleri boyutunda kadın üniversite öğrencileri ile erkek üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmıştır. Bu farkın etki büyüklüğü küçük düzeydedir. Çevrimiçi risk alma eğilimi ölçeğinin başkasına zarar verme riskleri boyutu ele alındığında ise kadın üniversite öğrencilerinin ortalaması (x̄=1,186), erkek üniversite öğrencilerinin ortalamasından (x̄= 1,430) daha yüksek olduğu görülmektedir ($t_{(980,432)}$ =-9,301; p<0,001; η^2=0,051). Bu durumda, çevrimiçi risk alma eğilimi ölçeğinin başkalarına zarar verme riskleri boyutunda kadın üniversite öğrencileri ile erkek üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmıştır. Bu farkın etki büyüklüğü ise orta düzeydedir. Sonuç olarak üniversite öğrencilerinin cinsiyetleri bağlamında, şimdiki çevrimiçi risk alma eğilimleri incelendiğinde

sosyalleşme riskleri, ticari riskler ve kişisel bilgileri açma riskleri eğilimleri erkeklerde kadınlara oranla daha yüksek olduğu görülürken, başkalarına zarar verme riskleri kadınlarda erkeklere oranla daha yüksek olduğu belirlenmiştir.

3.2.3. Üniversite öğrencilerinin geçmişteki çevrimiçi risk alma eğilimlerinin cinsiyete göre incelenmesi

Bu çalışmayla üniversite öğrencilerinden elde edilen veriler, birbirinden bağımsız iki grubun sürekli bir değişken üzerinden aldıkları ortalama puanların karşılaştırılmasını sağlayan bağımsız örneklemler için t testi ile analiz edilmiştir. Tablo 3.6'da görüldüğü gibi üniversite öğrencilerinin geçmişteki çevrimiçi risk alma eğilimleri cinsiyetlerine göre farklılaşıp farklılaşmadıkları incelenmiştir.

Tablo 3.6. *Üniversite öğrencilerinin geçmişteki çevrimiçi risk alma eğilimlerinin cinsiyete göre karşılaştırılması*

	Grup	n	x̄	ss	sd	t	p	η2
Sosyalleşme Riskleri	Kadın	975	2,027	,795	1595	-10,145	,000	0,061
	Erkek	622	2,441	,798				
Ticari Riskler	Kadın	975	1,422	,526	970,797	-21,982	,000	0,232
	Erkek	622	2,212	,792				
Kişisel Bilgileri Açma Riskleri	Kadın	975	2,183	,861	1595	-5,211	,000	0,017
	Erkek	622	2,416	,890				
Başkasına Zarar Verme Riskleri	Kadın	975	1,291	,485	1021,003	-9,631	,000	0,055
	Erkek	622	1,593	,680				

Tablo 3.6'da çevrimiçi risk alma eğilimi ölçeğinin sosyalleşme riskleri boyutunda kadın üniversite öğrencilerinin ortalaması ($\bar{x}$=2,027), erkek üniversite öğrencilerinin ortalamasından ($\bar{x}$= 2,441) daha düşük olduğu görülmektedir ($t_{(1595)}$ =-10,145; p<0,001; η^2=0,061). Yani çevrimiçi risk alma eğilimi ölçeğinin sosyalleşme riskleri boyutunda kadın üniversite öğrencileri ile erkek üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmıştır. Bu farkın etki büyüklüğü ise orta düzeydedir. Çevrimiçi risk alma eğilimi ölçeğinin ticari riskler boyutunda, sosyalleşme risklerinde olduğu gibi kadın üniversite öğrencilerinin ortalaması ($\bar{x}$=1,421), erkek üniversite öğrencilerinin ortalamasından ($\bar{x}$= 2,212) daha düşük olduğu görülmektedir ($t_{(970,797)}$ =-21,982; p<0,001; η^2=0,232). Bu durumda, çevrimiçi risk alma eğilimi ölçeğinin ticari riskler boyutunda

kadın üniversite öğrencileri ile erkek üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmıştır. Bu farkın etki büyüklüğü çok yüksek düzeydedir. Çevrimiçi risk alma eğilimi ölçeğinin kişisel bilgileri açma riskleri boyutunda kadın üniversite öğrencilerinin ortalaması ($\bar{x}$=2,182), erkek üniversite öğrencilerinin ortalamasından ($\bar{x}$= 2,416) daha düşük olduğu görülmektedir ($t_{(1595)}$ =-5,211; p<0,001; η^2=0,017). Bu durumda, çevrimiçi risk alma eğilimi ölçeğinin kişisel bilgileri açma riskleri boyutunda kadın üniversite öğrencileri ile erkek üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmıştır. Bu farkın etki büyüklüğü küçük düzeydedir. Çevrimiçi risk alma eğilimi ölçeğinin başkasına zarar verme riskleri boyutu ele alındığında ise kadın üniversite öğrencilerinin ortalaması ($\bar{x}$=1,290), erkek üniversite öğrencilerinin ortalamasından ($\bar{x}$= 1,592) daha düşük olduğu görülmektedir ($t_{(1021,003)}$ =-9,631; p<0,001; η^2=0,055). Bu durumda, çevrimiçi risk alma eğilimi ölçeğinin başkalarına zarar verme riskleri boyutunda kadın üniversite öğrencileri ile erkek üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmıştır. Bu farkın etki büyüklüğü ise orta düzeydedir. Sonuç olarak üniversite öğrencilerinin cinsiyetleri bağlamında, geçmişteki çevrimiçi risk alma eğilimleri incelendiğinde sosyalleşme riskleri, ticari riskler, kişisel bilgileri açma riskleri ve başkasına zarar verme riskleri eğilimleri erkeklerde kadınlara oranla daha yüksek bulgusuna ulaşılmıştır.

3.3. Yaş Gruplarına Göre Üniversite Öğrencilerinin Dijital Güvenlik Öz Yeterlik Düzeyleri ve Şimdiki Çevrimiçi Risk Alma Eğilimlerinin İncelenmesi

Bu bölümde üniversite öğrencilerinin yaş gruplarına göre dijital güvenlik öz yeterlik düzeyleri ve şimdiki çevrimiçi risk alma eğilimleri sunulmuştur. Verilerin yaş değişkeni çerçevesinde incelenmesi ve yorumlanması için yaş grupları oluşturulmuştur. Tablo 3.7 incelendiğinde üniversite öğrencilerinin yaşları 18 ile 39 arasında değişmektedir. Bu yaşlardaki öğrencilerin puanlarının karşılaştırılabilmeleri için yaş gruplarında bulunan öğrenci sayılarının karşılaştırılabilecek oranda olması gerekmektedir. Tablo 3.7'deki veriler incelendiğinde yaş gruplarındaki katılımcı sayılarının karşılaştırılamayacak oranda olduğu görülmüştür. Dolayısıyla yaş değişkeni üzerinde anlamlı ve alanyazın ile desteklenebilecek bir gruplama işlemi yapılması gerekmektedir. Tablo 4.7'de Üniversite öğrencilerinin cinsiyet ve yaşlarına göre dağılımı sunulmuştur. Bu araştırma kapsamında öncelikle 20 yaş ve altı, 21 ve 22 yaş, 23 yaş ve

üstü bireyler üç gruba ayrılarak cinsiyete göre bu yaş grupları arasında farkın olup olmadığının incelenmesi tek yönlü varyans analizi gerçekleştirilmiştir.

Tablo 3.7. *Üniversite öğrencilerinin cinsiyet ve yaşlarına göre dağılımı*

		Cinsiyet		Toplam
		Kadın	Erkek	
Yaş	18	55	18	73
	19	144	65	209
	20	237	99	336
	21	233	152	385
	22	127	116	243
	23	90	67	157
	24	44	43	87
	25	17	23	40
	26	12	16	28
	27	1	6	7
	28	2	7	9
	29	1	4	5
	30	1	0	1
	31	0	1	1
	34	1	0	1
	36	0	3	3
	37	0	1	1
	39	1	0	1
Toplam		966	621	1587

Bu analiz sonucunda 21 ve 22 yaş grubu ile 23 ve üstü yaş grubu arasında bir farkın olmadığı, 20 yaş ve altı grup ile diğer gruplar arasında anlamlı farkın olduğu ortaya çıkmıştır. Daha sonra yaş grupları 21 yaş ve altı 22 yaş ve 23 yaş ve üstü olacak şekilde bireyler yaş gruplarına ayrılmış ve yine cinsiyete göre tek yönlü varyans analizi işe koşulmuştur. Analiz sonucunda 22 yaş ve 23 yaş ve üstü olan yaş grupları arasında anlamlı bir fark çıkmazken, 21 yaş ve altı grubun diğer yaş grupları ile arasında anlamlı bir fark olduğu görülmüştür. Dolayısıyla araştırmanın yaş değişkeni ile incelenmesi için oluşturulan ve gruplarda kıyaslamaya engel olmayacak katılımcı sayıları olan 21 yaş ve altı ve 22 yaş ve üstü şeklinde iki grup oluşturulmuştur.

3.3.1. Üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeylerinin yaş gruplarına göre incelenmesi

Üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeylerini yaş gruplarına göre incelenmesi için ikiden fazla gruplarla bir bağımlı değişken arasında karşılaştırma yapmayı sağlayan tek yönlü varyans analizi kullanılması gerekmektedir. Bu doğrultuda üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri bağımsız örneklemler t testi

ile incelenmiştir. Tablo 3.8'de üniversite öğrencilerinin yaş grubuna göre dijital güvenlik öz yeterlik düzeylerinin karşılaştırılması sunulmuştur.

Tablo 3.8. *Üniversite öğrencilerinin yaş grubuna göre dijital güvenlik öz yeterlik düzeylerinin karşılaştırılması*

	Yaş Grubu	**n**	**x̄**	**ss**	**sd**	**t**	**p**	**η2**
Dijital uygulamalarda güvenlik	21 yaş ve altı	1006	4,556	,476	1589	-0,894	,371	-
	22 yaş ve üstü	585	4,579	,477				
Dijital araçlarda güvenlik	21 yaş ve altı	1006	3,830	,813	1589	-3,853	,000	0,008
	22 yaş ve üstü	585	3,989	,760				

Tablo 3.8 incelendiğinde, dijital güvenlik öz yeterlik ölçeğinin dijital uygulamalarda güvenlik alt boyutunun 21 yaş ve altı üniversite öğrencilerinin ortalaması ($\bar{x}$=4,556), ile 22 yaş ve üstü üniversite öğrencilerinin ortalamasının ($\bar{x}$=4,578) yüksek düzeyde olduğu görülmektedir ($t_{(1589)}$ =-0,894; p>0,05). Bu durumda, dijital güvenlik öz yeterlik ölçeğinin dijital uygulamalarda güvenlik becerileri boyutunda üniversite öğrencilerinin yaş grupları arasında istatistiksel olarak anlamlı bir fark çıkmamıştır. Dijital güvenlik öz yeterlik ölçeğinin dijital araçlarda güvenlik boyutunda ise 21 yaş ve altı üniversite öğrencilerinin ortalamasının ($\bar{x}$=3,829), 22 yaş ve üstü üniversite öğrencilerinin ortalamasından ($\bar{x}$=3,988) daha düşük olduğu görülmektedir ($t_{(1589)}$ =-3,853; p<0,001; η^2=0.008). Yani dijital güvenlik öz yeterlik ölçeğinin dijital araçlarda güvenlik boyutunda üniversite öğrencilerinin yaş grupları arasında istatistiksel olarak anlamlı ve küçük düzeyde bir fark çıkmıştır. Sonuç olarak üniversite öğrencilerinin dijital araçlarda güvenlik öz yeterlik düzeyleri 22 yaş ve üstü bireylerde 21 yaş ve altı bireylere oranla daha yüksek olduğu bulgusuna ulaşılmıştır.

3.3.2. Üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin yaş gruplarına göre incelenmesi

Üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin yaş değişkenine göre incelenebilmesi için yukarıdaki bölümde yapılan yaş değişkenine ilişkin analiz denemeleri çevrimiçi risk alma eğilimi ölçeği için tekrarlanmıştır. Bunun sonucunda yaş değişkeni, 21 yaş ve altı ve 22 yaş ve üstü olarak gruplandırılıp, bağımsız örneklemler t

testi analizine tabi tutulmuştur. Tablo 3.9'da üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin yaş gruplarına göre karşılaştırılması sunulmuştur.

Tablo 3.9. *Üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin yaş gruplarına göre karşılaştırılması*

	Yaş Grupları	n	x̄	ss	sd	t	p	η2
Sosyalleşme Riskleri	21 yaş ve altı	1006	1,929	,712	1589	-0,953	.341	-
	22 yaş ve üstü	585	1,965	,737				
Ticari Riskler	21 yaş ve altı	1006	1,794	,793	1589	-5,263	.000	.017
	22 yaş ve üstü	585	2,016	,842				
Kişisel Bilgileri Açma Riskleri	21 yaş ve altı	1006	2,315	,859	1589	1,826	.068	-
	22 yaş ve üstü	585	2,234	,852				
Başkasına Zarar Verme Riskleri	21 yaş ve altı	1006	1,280	,483	1589	-0,205	.838	-
	22 yaş ve üstü	585	1,286	,489				

Tablo 3.9'da çevrimiçi risk alma eğilimi ölçeğinin sosyalleşme riskleri boyutunda 21 yaş ve altı yaş grubundaki üniversite öğrencilerinin ortalaması (x̄=1,929) ile 22 yaş ve üstü yaş grubunda bulunan üniversite öğrencilerinin ortalamasının (x̄=1,965) birbirine oldukça yakın düzeyde olduğu görülmektedir ($t_{(1589)}$ =-0,953; p>0,05). Bu doğrultuda üniversite öğrencilerinin şimdiki sosyalleşme riskleri eğilimleri ile yaş grupları arasında istatistiksel olarak anlamlı bir fark çıkmamıştır. Çevrimiçi risk alma eğilimi ölçeğinin ticari riskler boyutunda, 21 yaş ve altı yaş grubundaki üniversite öğrencilerinin ortalaması (x̄=1,794), 22 yaş ve üstü yaş grubunda bulunan üniversite öğrencilerinin ortalamasından (x̄=2,016) daha düşük olduğu görülmektedir ($t_{(1589)}$ =-5,263; p<0,001; η^2=0,017). Bu durumda çevrimiçi risk alma eğilimi ölçeğinin ticari riskler boyutunda yaş grupları arasında istatistiksel olarak küçük düzeyde anlamlı bir fark çıkmıştır. Çevrimiçi risk alma eğilimi ölçeğinin kişisel bilgileri açma riskleri boyutunda 21 yaş ve altı yaş grubundaki üniversite öğrencilerinin ortalaması (x̄=2,315) ile 22 yaş ve üstü yaş grubunda bulunan üniversite öğrencilerinin ortalamasının (x̄=2,234) birbirine oldukça yakın düzeyde olduğu görülmektedir ($t_{(1589)}$ =1,826; p>0,05). Bu doğrultuda üniversite öğrencilerinin şimdiki kişisel bilgileri açma riskleri eğilimleri ile yaş grupları arasında istatistiksel olarak anlamlı bir fark çıkmamıştır. Çevrimiçi risk alma eğilimi ölçeğinin başkasına zarar verme

riskleri boyutunda 21 yaş ve altı yaş grubundaki üniversite öğrencilerinin ortalaması ($\bar{x}$=1,280) ile 22 yaş ve üstü yaş grubunda bulunan üniversite öğrencilerinin ortalamasının ($\bar{x}$=1,285) birbirine oldukça yakın düzeyde olduğu görülmektedir ($t_{(1589)}$=-0,205; p>0,05). Bu doğrultuda üniversite öğrencilerinin şimdiki başkasına zarar verme riskleri eğilimleri ile yaş grupları arasında istatistiksel olarak anlamlı bir fark çıkmamıştır. Sonuç olarak üniversite öğrencilerinin yaş grupları bağlamında, şimdiki sosyalleşme riskleri, kişisel bilgileri açma riskleri ve başkasına zarar verme riskleri bakımından eğilimleri 21 ve altı yaş ve 22 yaş ve üstü yaş gruplarında benzer olduğu belirlenirken, şimdiki ticari riskler eğilimleri 21 ve altı yaş grubunda, 22 ve üstü yaş grubuna oranla düşük olduğu bulgusuna ulaşılmıştır.

3.4. Bilim Dallarına Göre Üniversite Öğrencilerinin Dijital Güvenlik Öz Yeterlik Düzeyleri ve Şimdiki Çevrimiçi Risk Alma Eğilimlerinin İncelenmesi

Bu bölümde üniversite öğrencilerinin öğrenim gördükleri bilim dallarına göre dijital güvenlik öz yeterlik düzeyleri ve şimdiki çevrimiçi risk alma eğilimleri incelenmiş ve yorumlanmıştır.

3.4.1. Üniversite öğrencilerinin bilim dallarına göre dijital güvenlik öz yeterlikleri düzeylerinin incelenmesi

Üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeylerinin bilim dallarına göre incelenebilmesi için üniversite öğrencilerinin öğrenim gördükleri bölümler, Sosyal Bilim ve Fen Bilim dalları altında gruplandırılmıştır. Daha sonra veriler bağımsız gruplar t testi işe koşularak incelenmiştir. Tablo 3.10'da üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeylerinin öğrenim gördükleri bilim dallarına göre karşılaştırılması sunulmuştur.

Tablo 3.10. *Üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeylerinin öğrenim gördükleri bilim dallarına göre karşılaştırılması*

	Gruplar	**n**	**x̄**	**ss**	**sd**	**t**	**p**	**η2**
Dijital uygulamalarda güvenlik	Sosyal Bilimler	1000	4,529	,483	1579	-3,607	.000	.008
	Fen Bilimleri	581	4,619	,459				
Dijital araçlarda güvenlik	Sosyal Bilimler	1000	3,802	,805	1579	-5,448	.000	.018
	Fen Bilimleri	581	4,026	,758				

Tablo 3.10'da görüldüğü gibi dijital güvenlik öz yeterlik ölçeğinin dijital uygulamalarda güvenlik boyutu ele alındığında sosyal bilimler alanında öğrenim gören öğrencilerin ortalaması ($\bar{x}$=4,529), fen bilimleri alanında öğrenim gören öğrencilerin ortalamasından ($\bar{x}$=4,618) düşük olduğu görülmektedir ($t_{(1579)}$ =-3,607; p<0,001; η^2=0,008). Dijital güvenlik öz yeterlik ölçeğinin dijital uygulamalarda güvenlik boyutunda bilim dalları açısından istatistiksel olarak küçük düzeyde anlamlı bir fark çıkmıştır. Dijital güvenlik öz yeterlik ölçeğinin dijital araçlarda güvenlik boyutu ele alındığında sosyal bilimler alanında öğrenim gören öğrencilerin ortalaması ($\bar{x}$=3,802), fen bilimleri alanında öğrenim gören öğrencilerin ortalamasından ($\bar{x}$=4,026) düşük olduğu görülmektedir ($t_{(1579)}$ =-5,448; p<0,001; η^2=.018). Bu doğrultuda dijital güvenlik öz yeterlik ölçeğinin dijital araçlarda güvenlik boyutunda bilim dalları açısından istatistiksel olarak küçük düzeyde anlamlı bir fark çıkmıştır. Sonuç olarak üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri öğrenim gördükleri bilim dallarına göre farklılaştığı ve fen bilimlerinde öğrenim gören üniversite öğrencilerinin sosyal bilimlerdekilere oranla dijital güvenlik öz yeterlik düzeylerinin yüksek olduğu belirlenmiştir.

3.4.2. Üniversite öğrencilerinin bilim dallarına göre şimdiki çevrimiçi risk alma eğilimlerinin incelenmesi

Üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin bilim dallarına göre incelenebilmesi için üniversite öğrencilerinin öğrenim gördükleri bölümler, sosyal bilim ve fen bilim dalları altında gruplandırılmıştır. Daha sonra veriler bağımsız gruplar t testi işe koşularak incelenmiştir. Tablo 4.11'de üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin öğrenim gördükleri bilim dallarına göre karşılaştırılması sunulmuştur. Tablo 4.11'de çevrimiçi risk alma eğilimi ölçeğinin şimdiki sosyalleşme riskleri alt boyutunda sosyal bilimlerde öğrenim gören üniversite öğrencilerinin ortalaması ($\bar{x}$=1,871), fen bilimlerinde öğrenim gören üniversite öğrencilerinin ortalamasından ($\bar{x}$=1,844) daha yüksek olduğu görülmektedir ($t_{(1579)}$ =2,864; p<0,05; η^2=0,005). Çevrimiçi risk alma eğilimi ölçeğinin sosyalleşme riskleri boyutunda sosyal bilimlerde öğrenim gören üniversite öğrencileri ile fen bilimlerinde öğrenim gören üniversite öğrencileri arasında küçük düzeyde istatistiksel olarak anlamlı bir fark çıkmıştır. Tablo 3.11'de görüldüğü gibi, çevrimiçi risk alma eğilimi ölçeğinin şimdiki ticari riskler alt boyutunda sosyal bilimlerde öğrenim gören üniversite öğrencilerinin ortalaması ($\bar{x}$=1,912), fen bilimlerinde öğrenim gören üniversite öğrencilerinin

ortalamasından ($\bar{x}$=2,315) düşük olduğu görülmektedir ($t_{(1579)}$ =-1,603; p>0,05). Bu durumda çevrimiçi risk alma eğilimi ölçeğinin ticari riskler boyutunda sosyal bilimlerde öğrenim gören üniversite öğrencileri ile fen bilimlerinde öğrenim gören üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmamıştır.

Tablo 3.11. *Üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin öğrenim gördükleri bilim dallarına göre karşılaştırılması*

	Gruplar	**n**	**$\bar{x}$**	**ss**	**sd**	**t**	**p**	**η2**
Sosyalleşme Riskleri	Sosyal Bilimler	1000	1,871	,722	1579	2,864	,004	0,005
	Fen Bilimleri	581	1,844	,709				
Ticari Riskler	Sosyal Bilimler	1000	1,912	,821	1579	-1,603	,109	-
	Fen Bilimleri	581	2,315	,805				
Kişisel Bilgileri Açma Riskleri	Sosyal Bilimler	1000	2,217	,870	1579	2,189	,029	0,003
	Fen Bilimleri	581	1,265	,834				
Başkasına Zarar Verme Riskleri	Sosyal Bilimler	1000	1,305	,464	1118,424	-1,550	,121	-
	Fen Bilimleri	581	1,871	,512				

Tablo 3.11 incelendiğinde, çevrimiçi risk alma eğilimi ölçeğinin kişisel bilgileri açma riskleri boyutunda sosyal bilimlerde öğrenim gören üniversite öğrencilerinin ortalaması ($\bar{x}$=2,217), fen bilimlerinde öğrenim gören üniversite öğrencilerinin ortalamasından ($\bar{x}$=1,265) daha yüksek olduğu görülmektedir ($t_{(1579)}$ =2,189; p<0,05; η^2=0,003). Yani çevrimiçi risk alma eğilimi ölçeğinin kişisel bilgileri açma riskleri boyutunda sosyal bilimlerde öğrenim gören üniversite öğrencileri ile fen bilimlerinde öğrenim gören üniversite öğrencileri arasında küçük düzeyde istatistiksel olarak anlamlı bir fark çıkmıştır. Çevrimiçi risk alma eğilimi ölçeğinin şimdiki başkasına zarar verme riskleri boyutunda sosyal bilimlerde öğrenim gören üniversite öğrencilerinin ortalaması ($\bar{x}$=1,305), fen bilimlerinde öğrenim gören üniversite öğrencilerinin ortalamasından ($\bar{x}$=1,871) düşük olduğu görülmektedir ($t_{(1118,424)}$ =-1,550; p>0,05). Bu durumda çevrimiçi risk alma eğilimi ölçeğinin başkalarına zarar verme riskleri boyutunda sosyal bilimlerde öğrenim gören üniversite öğrencileri ile fen bilimlerinde öğrenim gören üniversite öğrencileri arasında istatistiksel olarak anlamlı bir fark çıkmamıştır. Sonuç olarak şimdiki çevrimiçi risk alma eğilimi ölçeği boyutlarından ticari riskler ile başkasına zarar verme riskleri eğilimleri bakımından üniversite öğrencilerinin öğrenim gördükleri

bilim dallarına göre bir farklılık olmazken, sosyal bilimlerde öğrenim gören üniversite öğrencilerinin, fen bilimlerinde öğrenim gören üniversite öğrencilerine oranla sosyalleşme riskleri ve kişisel bilgilerini açma riskleri eğilimlerinin daha yüksek olduğu belirlenmiştir.

3.5. İnternet Kullanım Sıklıklarına Göre Üniversite Öğrencilerinin Dijital Güvenlik Öz Yeterlik Düzeyleri ve Şimdiki Çevrimiçi Risk Alma Eğilimlerinin İncelenmesi

Bu bölümde üniversite öğrencilerinin internet kullanım sıklıklarına göre dijital güvenlik öz yeterlik düzeyleri ve şimdiki çevrimiçi risk alma eğilimleri incelenmiş ve yorumlanmıştır. Üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri ve şimdiki çevrimiçi risk alma eğilimlerinin internet kullanım sıklıklarına göre incelemek için ikiden fazla gruplarla bir bağımlı değişken arasında karşılaştırma yapmayı sağlayan tek yönlü varyans analizi kullanılması gerekmektedir. Tablo 3.12'de üniversite öğrencilerinin internet kullanım sıklıkları sunulmuştur.

Tablo 3.12. *Üniversite öğrencilerinin internet kullanım sıklıkları*

İnternet Kullanım Sıklığı	f	%
Haftada 0-2 saat	16	1,0
Haftada 2-5 saat	40	2,5
Günde 0-3 saat	218	13,6
Günde 3-5 saat	753	47,0
Günde 5-7 saat	490	30,6
Diğer*	75	4,7
Toplam	1592	99,4
Belirtilmemiş	9	,6
Toplam	1601	100,0

* Diğer grubundaki bireyler genellikle günde 10 saat ve üstü internet kullanıcısı olduğunu belirtmişlerdir.

Tablo 3.12 incelendiğinde üniversite öğrencilerinin internet kullanım sıklıklarının "Günde 3-5 saat" ve "Günde 5-7 saat" aralıklarında yoğunlaştığı görülmektedir. Dolayısıyla bu aralıklar tekrar gruplandırılarak analize tabi tutulmuştur. Artık internet kullanıcılarına haftalık internet kullanım bilgisinin sorulması yerine günlük internet kullanım sıklığını belirtmeleri araştırmacılar için daha anlamlı bir veri olacaktır. Dolayısıyla internet kullanım sıklığı değişkeni üç grup altında toplanmıştır. Bunlar "Günde 3 saat ve altı" Günde 3-5 saat" ve "Günde 5 saat ve üstü" olarak isimlendirilmiştir.

3.5.1. Üniversite öğrencilerinin dijital öz yeterlik düzeylerinin internet kullanım sıklıklarına göre incelenmesi

Üniversite öğrencilerinin internet kullanım sıklıkları kullanılarak yapılan analizlerde tek yönlü varyans analizi işe koşulmuştur. Tablo 3.13'te üniversite öğrencilerinin dijital güvenlik öz yeterlikv düzeylerinin internet kullanım sıklıklarına göre karşılaştırılması sunulmuştur.

Tablo 3.13. *Üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeylerinin internet kullanım sıklıklarına göre karşılaştırılması*

	Varyansın Kaynağı	KT	sd	KO	F	p	η2
Dijital uygulamalarda güvenlik	Gruplar arası	3,308	2	1,654	7,270	,001	0,009
	Gruplar içi	361,500	1589	,228			
	Toplam	364,808	1591				
Dijital araçlarda güvenlik	Gruplar arası	4,081	2	2,040	3,221	,040	0,004
	Gruplar içi	1006,419	1589	,633			
	Toplam	1010,499	1591				

Tablo 3.13'teki analiz sonuçlarına bakıldığında üniversite öğrencilerinin dijital güvenlik öz yeterlik ölçeğinin dijital uygulamalarda güvenlik boyutunda ($F_{(2,1589)}$ =7,270; $p<0,05$; η^2=0,009) ve dijital araçlarda güvenlik boyutunda ($F_{(2,1589)}$ =3,221; $p<0,05$; η^2=0,004) internet kullanım sıklıklarına bağlı olarak istatistiksel olarak anlamlı bir farklılık gösterdiği görülmüştür. Ancak istatistiksel farklılığın etki büyüklüklerinin ise küçük düzeyde olduğu görülmektedir. Söz konusu farklılığın hangi gruplar arasından kaynaklandığını belirlemek için varyans eşteşliğinin sağlandığı durumlarda incelenebilen Post-Hoc testlerinden Scheffe ve varyans eşteşliğinin sağlanamadığı durumlarda incelenebilen Post-Hoc testlerinden Tamhane testi kullanılmıştır. Dijital uygulamalarda güvenlik boyutu ele alındığında Tamhane testi sonucuna göre farklılık, günde 5 saat ve üstü internet kullanım sıklığına sahip üniversite öğrencileri ile günde 3 saat ve altı internet kullanım sıklığına sahip üniversite öğrencileri grupları arasında kaynaklandığı, günde 5 saat ve üstü sıklığında internet kullanana üniversite öğrencilerinin ortalamalarının diğer gruba oranla yüksek olduğu ortaya çıkmıştır. Dijital araçlarda güvenlik boyutu ele alındığında ise Scheffe testi sonucuna göre günde 5 saat ve üstü internet kullanım sıklığına sahip üniversite öğrencileri ile günde 3 saat ve altı internet kullanım sıklığına

sahip üniversite öğrencileri grupları arasında kaynaklandığı, günde 5 saat ve üstü sıklığında internet kullanana üniversite öğrencilerinin ortalamalarının diğer gruba oranla yüksek olduğu ortaya çıkmıştır. Sonuç olarak günde 5 saat ve üstü internet kulanım sıklığına sahip üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri günde 3 saat ve altı sıklığında internet kullanan üniversite öğrencilerine göre daha yüksektir.

3.5.2. Üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin internet kullanım sıklıklarına göre incelenmesi

Üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerini internet kullanım sıklıklarına göre incelemek için ikiden fazla gruplarla bir bağımlı değişken arasında karşılaştırma yapmayı sağlayan tek yönlü varyans analizi işe koşulmuştur. Tablo 3.14'te üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin internet kullanım sıklıklarına göre karşılaştırılması sunulmuştur.

Tablo 3.14. *Üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinin internet kullanım sıklıklarına göre karşılaştırılması*

	Varyansın Kaynağı	KT	sd	KO	F	p	η2
Sosyalleşme Riskleri	Gruplar arası	10,342	2	5,171	10,048	,000	0,012
	Gruplar içi	817,725	1589	,515			
	Toplam	828,067	1591				
Ticari Riskler	Gruplar arası	11,329	2	5,664	8,553	,000	0,010
	Gruplar içi	1052,298	1589	,662			
	Toplam	1063,627	1591				
Kişisel Bilgileri Açma Riskleri	Gruplar arası	5,925	2	2,963	4,052	,018	0,005
	Gruplar içi	1161,818	1589	,731			
	Toplam	1167,743	1591				
Başkasına Zarar Verme Riskleri	Gruplar arası	1,320	2	,660	2,812	,060	-
	Gruplar içi	372,972	1589	,235			
	Toplam	374,292	1591				

Tablo 3.14 incelendiğinde üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimi ölçeğinin sosyalleşme riskleri ($F_{(2,1589)}$ =10,048; p<0,001; η^2=0,012), ticari riskler ($F_{(3,1589)}$ =8,553; p<0,001; η^2=0,010) ve kişisel bilgileri açma riskleri ($F_{(3,1589)}$ =4,052; p<0,05; η^2=0,005) boyutlarında, internet kullanım sıklıklarına göre küçük düzeyde anlamlı farklılık gösterdiği, fakat başkasına zarar verme riskleri boyutunda ($F_{(3,1589)}$ =2,812; p>0,05) ise internet kullanım sıklıklarına göre istatistiksel olarak anlamlı bir farklılık göstermediği görülmüştür. Söz konusu anlamlı farklılıkların hangi gruplar arasından kaynaklandığını belirlemek için varyans eşteşliğinin sağlanamadığı durumlarda

incelenebilen Post-Hoc testlerinden Tamhane testi işe koşulmuştur. Şimdiki sosyalleşme riskleri boyutunda Tamhane testine göre, üniversite öğrencilerinin günde 5 saat ve üstü internet kullanım sıklığına sahip olanlar ile günde 3-5 saat ve günde 3 saat ve altı sıklıklarında internet kullanım sıklığı olan gruplardan bu farklılığın kaynaklandığı, günde 5 saat ve üstü sıklığında internet kullanan üniversite öğrencilerinin ortalamalarının diğerlerine oranla yüksek olduğu ortaya çıkmıştır. Şimdiki ticari riskler boyutu ele alındığında Tamhane testi sonucuna göre, üniversite öğrencilerinin günde 5 saat ve üstü internet kullanım sıklığına sahip olanlar ile günde 3-5 saat ve günde 3 saat ve altı sıklıklarında internet kullanım sıklığı olan gruplardan bu farklılığın kaynaklandığı, günde 5 saat ve üstü sıklığında internet kullanan üniversite öğrencilerinin ortalamalarının diğerlerine oranla yüksek olduğu ortaya çıkmıştır. Şimdiki kişisel bilgileri açma riskleri boyutu ele alındığında Tamhane testi sonucuna göre, günde 5 saat ve üstü internet kullanım sıklığına sahip olanlar ile günde 3 saat ve altı internet kullanım sıklığı olan gruplardan bu farklılığın kaynaklandığı, günde 5 saat ve üstü sıklığında internet kullanan üniversite öğrencilerinin ortalamalarının diğer gruba oranla yüksek olduğu belirlenmiştir.

3.6. Üniversite Öğrencilerinin Dijital Güvenlik Öz Yeterlik Düzeyleri ile Şimdiki ve Geçmişteki Çevrimiçi Risk Alma Eğilimleri Arasındaki İlişkilerin İncelenmesi

Üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri, şimdiki ve geçmişteki çevrimiçi risk alma eğilimleri arasındaki ilişkilerin güçleri ve yönlerinin nasıl olduğunun incelenmesi için korelasyon analiz türü işe koşulmuştur. Tablo 3.15'de üniversite öğrencilerinin dijital güvenlik öz yeterlik, şimdiki çevrimiçi risk alma eğilimi ölçeği boyutları ve geçmişteki çevrimiçi risk alma eğilimleri arasındaki ilişkiler sunulmuştur. Tablo 3.15 incelendiğinde, üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri, şimdiki çevrimiçi risk alma eğilimleri ve geçmişteki çevrimiçi risk alma eğilimleri arasında istatistiksel olarak anlamlı veya anlamsız ilişkiler bulunduğu görülmektedir. Dijital güvenlik öz yeterlik ölçeğinin dijital uygulamalarda güvenlik boyutu ile çevrimiçi risk alma eğilimleri ölçeği şimdiki ticari riskler (r=.085; p=.001), şimdiki başkasına zarar verme riskleri (r=-.109; p=.000), geçmişteki ticari riskler (r=.072; p=.004) ve geçmişteki başkasına zarar verme riskleri (r=.072; p=.004) boyutlarıyla aralarında istatistiksel olarak anlamlı bağıntı katsayıları vardır. İki değişken arasındaki ilişki katsayısının gücü için Cohen (1988), ,10-,29 aralığındaki değerlerin küçük, ,30-,49

aralığındaki değerlerin orta ve ,50-1,0 aralığındaki değerlerin ise büyük kuvvette oluğunu belirtmektedir.

Tablo 3.15. *Üniversite öğrencilerinin dijital güvenlik öz yeterlikleri, şimdiki çevrimiçi risk alma eğilimi ölçeği boyutları ve geçmişteki çevrimiçi risk alma eğilimleri arasındaki ilişkiler*

n=1601	Dijital Uygulamalarda güvenlik	Dijital Araçlarda Güvenlik	Şimdiki Sosyalleşme Riskleri	Şimdiki Ticari Riskler	Şimdiki Kişisel Bilgileri Açma Riskleri	Şimdiki Başkasına Zarar Verme Riskleri	Geçmişteki Sosyalleşme Riskleri	Geçmişteki Ticari Riskler	Geçmişteki Kişisel Bilgileri Acma Riskleri
Dijital Araçlarda Güvenlik	,577**	-							
Şimdiki Sosyalleşme Riskleri	-,011	,109**	-						
Şimdiki Ticari Riskler	,085**	,235**	,409**	-					
Şimdiki Kişisel Bilgileri Açma Riskleri	-,025	-,044	,411**	,311**	-				
Şimdiki Başkasına Zarar Verme Riskleri	-,109**	,057*	,373**	,411**	,299**	-			
Geçmişteki Sosyalleşme Riskleri	,026	,078**	,539**	,341**	,305**	,226**	-		
Geçmişteki Ticari Riskler	,072**	,243**	,381**	,784**	,243**	,400**	,385**	-	
Geçmişteki Kişisel Bilgileri Açma Riskleri	-,003	-,027	,297**	,264**	,769**	,238**	,484**	,340**	-
Geçmişteki Başkasına Zarar Verme Riskleri	-,072**	,049	,310**	,397**	,254**	,701**	,391**	,457**	,358**

** Korelasyon .001 düzeyinde anlamlıdır.
* Korelasyon .05 düzeyinde anlamlıdır.

Tablo 3.15'te görüldüğü gibi, üniversite öğrencilerinin dijital uygulamalarda güvenlik öz yeterlikleri ile şimdiki ticari riskler, geçmişteki ticari riskler ve geçmişteki başkasına zarar verme riskleri eğilimleri arasında pozitif yönde küçük kuvvette ilişkiye sahiptir. Bunun yanında üniversite öğrencilerinin dijital uygulamalarda güvenlik öz yeterlikleri ile şimdiki başkasına zarar verme riskleri eğilimi ile negatif yönde küçük kuvvette bir ilişkiye sahiptir.

Dijital güvenlik öz yeterlik ölçeğinin dijital araçlarda güvenlik boyutu ile çevrimiçi risk alma eğilimi ölçeği şimdiki sosyalleşme riskleri (r=.109; p=.000), şimdiki ticari riskler (r=.235; p=.000), şimdiki başkasına zarar verme riskleri (r=.057; p=.022) ve geçmişteki sosyalleşme riskleri (r=.078; p=.002) ve geçmişteki ticari riskler (r=.243; p=.000) boyutlarıyla aralarında küçük kuvvette ve pozitif yönde anlamlı bağıntı katsayıları vardır.

Çevrimiçi risk alma eğilimi ölçeğinin şimdiki sosyalleşme riskleri boyutunun, geçmişteki sosyalleşme riskleri (r=.539; p=.000) ile yüksek kuvvette, geçmişteki ticari riskler (r=.381; p=.000) ile orta kuvvette, geçmişteki kişisel bilgileri açma riskleri (r=.297; p=.000) ile küçük kuvvette ve geçmişteki başkasına zarar verme riskleri (r=.310; p=.000) ile orta kuvvette ve pozitif yönde anlamlı bağıntı katsayıları vardır.

Çevrimiçi risk alma eğilimi ölçeğinin şimdiki ticari riskler boyutunun, geçmişteki sosyalleşme riskleri (r=.341; p=.000) ile orta kuvvette, geçmişteki ticari riskler (r=.784; p=.000) ile yüksek kuvvette, geçmişteki kişisel bilgileri açma riskleri (r=.264; p=.000) ile düşük kuvvette ve geçmişteki başkasına zarar verme riskleri (r=.397; p=.000) ile orta kuvvette ve pozitif yönde istatistiksel olarak anlamlı bağıntı katsayısı vardır.

Çevrimiçi risk alma eğilimi ölçeği şimdiki kişisel bilgileri açma riskleri boyutunun, geçmişteki sosyalleşme riskleri (r=.305; p=.000) ile orta kuvvette, geçmişteki ticari riskler (r=.243; p=.000) ile küçük kuvvette, geçmişteki kişisel bilgileri açma riskleri (r=.769; p=.000) ile yüksek kuvvette ve geçmişteki başkasına zarar verme riskleri (r=.254; p=.000) ile düşük kuvvette ve pozitif yönde istatistiksel olarak anlamlı bir bağıntı katsayısı vardır.

Çevrimiçi risk alma eğilimi ölçeği şimdiki başkasına zarar verme riski boyutunun, geçmişteki sosyalleşme riskleri (r=.226; p=.000) ile küçük kuvvette, geçmişteki ticari riskler (r=.400; p=.000) ile orta kuvvette, geçmişteki kişisel bilgileri açma riskleri (r=.238; p=.000) ile küçük kuvvette ve geçmişteki başkasına zarar verme riskleri (r=.701; p=.000) ile yüksek kuvvette ve pozitif yönde istatistiksel olarak anlamlı bağıntı katsayısı vardır.

Sonuç olarak üniversite öğrencilerinin geçmişteki çevrimiçi risk alma eğilimleri arttıkça şimdiki çevrimiçi risk alma eğilimleri de artmaktadır. Bir sonraki başlıkta üniversite öğrencilerinin geçmiş çevrimiçi risk alma eğilimlerinin, şimdiki çevrimiçi risk alma eğilimleri ile ilişkisi incelenmiştir.

3.7. Üniversite Öğrencilerinin Geçmişteki Çevrimiçi Risk Alma Eğilimleri Boyutlarının Şimdiki Çevrimiçi Risk Alma Eğilimleri ile İlişkisi

Üniversite öğrencilerinin geçmişteki çevrimiçi risk alma eğilimleri boyutları olan geçmişteki sosyalleşme riskleri, ticari riskler, kişisel bilgileri açma riskleri ve başkasına zarar verme risklerinin şimdiki çevrimiçi risk alma eğilimlerinin nasıl yordandığını incelemek amacıyla çoklu doğrusal regresyon analizi işe koşulmuştur. Çoklu doğrusal regresyon analizinin yöntemi olarak ise aşamalı çoklu doğrusal regresyon analizi yöntemi kullanılmıştır. Bunun nedeni ise yordayıcı değişkenlerin yordanan değişken üzerinde anlamlı etkiye sahip olmaları, bir başka deyişle bağımlı değişkenle en yüksek korelasyonu gösteren bağımsız değişkenlerin eşitliğe alınmasıdır. Analize dijital güvenlik öz yeterlik düzeyleri boyutlarından olan dijital araçlarda güvenlik ve dijital uygulamalarda güvenlik değişkenleri, geçmişteki çevrimiçi risk alma eğilimi boyutları olan, sosyal riskler, ticari riskler, kişisel bilgileri açma riskleri ve başkasına zarar verme riskleri değişkenleri tabi tutulmuştur. Analiz sonucunda ise aşamalı çoklu regresyon yöntemine göre eşitlikte Tablo 3.16'da görüldüğü gibi geçmişteki ticari riskler, kişisel bilgileri açma riskleri ve başkasına zarar verme riskleri kalmıştır.

Tablo 3.16. *Üniversite öğrencilerinin geçmişteki çevrimiçi risk alma eğilimi boyutları tarafından şimdiki çevrimiçi risk alma eğilimlerinin yordanması*

Model	Yordayan Değişkenler	B	SH_B	β	ΔR^2
1	(Sabit)	1,146	,027		,350**
	Geçmişteki ticari riskler	,423	,014	,592**	
2	(Sabit)	,733	,030		,513**
	Geçmişteki ticari riskler	,319	,013	,446**	
	Geçmişteki kişisel bilgileri açma riskleri	,261	,011	,429**	
3	(Sabit)	,638	,030		,541**
	Geçmişteki ticari riskler	,267	,014	,374**	
	Geçmişteki kişisel bilgileri açma riskleri	,234	,011	,385**	
	Geçmişteki başkasına zarar verme riskleri	,174	,018	,191**	
4	(Sabit)	,565	,031		,557**
	Geçmişteki ticari riskler	,247	,014	,346**	
	Geçmişteki kişisel bilgileri açma riskleri	,201	,012	,330**	
	Geçmişteki başkasına zarar verme riskleri	,149	,018	,164**	
	Geçmişteki sosyalleşme riskleri	,100	,013	,153**	

** p<.001
Yordanan değişken: Şimdiki Çevrimiçi Risk Alma Eğilimi

Aşamalı regresyon analizi sonuçları Tablo 3.16'da görülmektedir. Analiz dört aşamada tamamlanmıştır. Analize birinci aşamada üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimlerinde, %35 ile en fazla varyansı açıklayan geçmişteki ticari

riskler değişkeni girmiştir. Analize sırasıyla ikinci aşamada varyansa %16 katkı ile geçmişteki kişisel bilgileri açma değişkeni, üçüncü aşamada %3 katkı ile geçmişteki başkasına zarar verme riskleri ve dördüncü aşamada %1 katkı ile geçmişteki sosyalleşme riskleri değişkenleri dahil olarak, açıklanan varyans %55'e yükselmiştir. Üniversite öğrencilerinin şimdiki risk alma eğilimleri ile geçmişteki ticari riskler, geçmişteki kişisel bilgileri açma riskleri, geçmişteki başkasına zarar verme riskleri ve geçmişteki sosyalleşme riskleri ile arasında pozitif ilişkiler vardır. Üniversite öğrencilerinin geçmişteki çevrimiçi risk alma eğilimleri arttıkça şimdiki çevrimiçi risk alma eğilimleri de artmaktadır.

4. SONUÇ, TARTIŞMA VE ÖNERİLER

Bu bölümde, araştırmaya ilişkin sonuçlar ve bu sonuçların alanyazındaki diğer bilimsel çalışmaların sonuçlarıyla olan benzerlik ve farklılıkları ilişkilendirilerek sunulmuştur.

4.1. Sonuç

Bu çalışmayla, üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri ve çevrimiçi risk alma eğilimleri belirlenerek, bu özelliklerinin cinsiyet, yaş grupları, bilim dalları ve internet kullanım sıklıkları gibi çeşitli değişkenler tarafından incelenmesi amaçlanmıştır. Bunun yanında dijital güvenlik öz yeterlik düzeyleri ile çevrimiçi risk alma eğilimleri arasındaki ilişkiler ve geçmiş çevrimiçi risk alma eğilimi boyutlarının şimdiki çevrimiçi risk alma eğilimini nasıl yordadığı belirtilmiştir. Araştırmada dijital güvenlik öz yeterlik ve çevrimiçi risk alma eğilimi ölçekleri geliştirilmiş, bu ölçeklerin geçerlik ve güvenirlik çalışmaları yapılmıştır. Verilerin analizinde betimsel ve çıkarımsal istatistik tekniklerinden yararlanılmış ve sonuçlar bu istatistiklere göre yorumlanmıştır. Genel olarak üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeylerinin yüksek olduğu, geçmişteki ve şimdiki çevrimiçi risk alma eğilimlerinin düşük düzeyde olduğu belirlenmiştir. Dijital güvenlik öz yeterlik ve çevrimiçi risk alma eğilimleri üzerinde cinsiyet, internet kullanım sıklıkları ve bilim dallarına göre anlamlı farklılıklar bulunmuştur. Üniversite öğrencilerinin dijital güvenlik öz yeterlik boyutları ile çevrimiçi risk alma eğilimi boyutları arasında anlamlı ilişkilerin olduğu ortaya çıkmış, aynı zamanda geçmişteki çevrimiçi risk alma eğilimleri boyutlarının, şimdiki çevrimiçi risk alma eğilimlerini yordadığı bulgularına ulaşılmıştır.

4.2. Tartışma

Bu çalışmada üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri irdelendiğinde dijital uygulamalarda güvenlik öz yeterlik düzeylerinin dijital araçlarda güvenlik öz yeterlik düzeylerinden daha yüksek olduğu ortaya çıkmıştır. Bunun nedeni üniversite öğrencilerinin, dijital uygulamalarda güvenliği sağlama konusundaki farkındalıklarının dijital araçlardaki güvenlik farkındalıklarından daha yüksek olması olabilir. Calvani, Fini, Ranieri ve Picci (2012), 14-16 yaş aralığındaki ergen bireylerle yaptıkları çalışmada, bu bireylerin dijital becerilerinin temel teknik becerilerden öteye gidemediğini, teknolojinin kavramsal anlayışı ile ilgili sosyo-ilişkisel bilgi ve yüksek

düzeyde bilişsel beceriler gerektiren daha önemli bilgi ve becerilere sahip olunması gerektiğini belirtmektedir. Çünkü bu çalışma sonucundan farklı olarak, gençlerin çevrimiçi davranışlarında kendi güvenliklerini sağlamaları konusundaki farkındalıklarının oldukça düşük olduğu görülmüştür. Livingstone ve diğ., (2011)'in 25 Avrupa ülkesinde yürüttükleri büyük ölçekli araştırmada, dijital güvenlik becerileri konusunda çocukları korumak için tasarlanan özelliklerin birçok genç ve bazı büyük yaştaki çocuklar tarafından anlaşılamadığı belirtilmiştir.

Üniversite öğrencilerinin şimdiki çevrimiçi risk alma eğilimine bakıldığında kişisel bilgilerini açma ve sosyalleşme riskleri boyutlarında, ticari riskler ve başkalarına zarar verme risklerinden daha fazla riskli davranış eğilimi gösterdikleri, geçmiş çevrimiçi risk alma eğiliminde de ilgili boyutlarda benzer riskli davranış eğilimi gösterdikleri ortaya çıkmıştır. Bunun nedeni kişisel bilgileri açma ve sosyalleşme riskleri hakkındaki risk algıları ticari riskler ve başkasına zarar verme riskleri algılarından daha farklı olması olabilir. Çünkü De Kimpe, Walrave, Hardyns, Pauwels ve Ponnet (2018) çalışmasında, çevrimiçi ödeme yapma, ya da çevrimiçi alışveriş yapma davranışının kimlik avı hedefi olmayı arttırdığını belirtmiştir. Bu gibi örneklerle karşılaşan bireyler, çevrimiçi ortamlarda ödeme yapma, alışveriş yapma gibi davranışları daha fazla riskli olarak algılamaları olabilir. Buna ek olarak üniversite öğrencilerinin geçmiş ve şimdiki çevrimiçi risk alma eğilimi incelendiğinde, geçmişte aldıkları sosyalleşme riskleri, şimdiki sosyalleşme risklerinden daha fazla olduğu sonucuna ulaşılmıştır. Bunun nedeni çocukluk dönemindeki bireylerin çeşitli internet tehditleri karşısında zarar-yarar dengesini kuramamaları ve kişisel bilgilerini açmanın ve sosyalleşme riskleri boyutundaki davranışları sergilemenin gelecekte onlara ne gibi zararlar getirebileceğini mantık süzgecinden geçirememeleri olabilir. Ayrıca üniversite öğrencilerinin hem geçmiş ve hem şimdiki ticari riskler konusunda az risk alma eğilimi göstermelerindeki etkenler, bu bireylerin ekonomik olarak ebeveynlerine bağlı olmaları ve sosyal medya, forumlar, ilgi toplulukları, sohbet odaları gibi kendilerini temsil eden elektronik hesap oluşturdukları ve başkaları ile iletişim kurdukları platformların veya e-ticaret ya da e alışveriş yaptıkları hizmetlerin sosyalleşme hizmetlerinden daha sonra yaygınlaşmaya başlaması olabilir. Başkalarına zarar verme risk eğilimleri başta olmak üzere diğer tüm risk eğilimi faktörlerindeki davranışları gösterme sıklıklarını az olarak belirtmelerinin nedeninin sosyal beğenirlikten etkilenmeleri ve öz bildirime dayalı olarak verdikleri bu yanıtların gerçekte daha fazla göstermeleri diğer nedenler arasında sayılabilir. Çünkü

Dönmez ve Akbulut (2016), siber zorbalık gibi öz bildirim yoluyla ölçülebilen hassas konularda sosyal beğenirlik potansiyelinin dikkate alınması gerektiği belirtilmiştir. Çevrimiçi risk alma eğilimi de siber zorbalık gibi hassas bir konu olarak düşünülebilir. Çünkü çevrimiçi riskler bağlamında sosyal medyada kişisel bilgilerin ifşası konusunda bireylerin kişisel bilgilerini paylaşma davranışına ilişkin niyetleri ile gerçek davranışları arasındaki ilişki bir paradoks olarak ele alınmıştır (Norberg, Horne ve Horne, 2007). Aynı zamanda yaşanan örnek olaylar incelendiğinde, çevrimiçi dolandırılma, çevrimiçi uygunsuz içerikler edinme veya oluşturma, başkalarını çevrimiçi ortamlarda gizli olarak takip etme gibi çeşitli çevrimiçi riskli davranışların arttığı, fakat bireylerin bu gibi davranışlarla karşılaşma ya da bu davranışları sergileme durumlarını ise az sıklıkta gösterdiklerini belirttikleri dikkat çekmektedir.

Üniversite öğrencilerinin cinsiyete göre dijital güvenlik öz yeterlik düzeyleri ele alındığında kadın ve erkek katılımcılarda yüksek düzeyde olduğu ortaya çıkmıştır. Dijital güvenlik öz yeterlik düzeyleri alt boyutlar çerçevesinde incelendiğinde ise dijital uygulamalarda üniversite öğrencilerinin cinsiyete göre değişmediği fakat dijital araçlarda güvenlik öz yeterlik düzeyleri cinsiyete göre değiştiği, erkeklerin kadınlara oranla daha yüksek dijital araçlarda güvenlik öz yeterlik düzeyine sahip olduğu sonucu ortaya çıkmıştır. Gratian, Bandi, Cukier, Dykstra ve Ginther (2018) üniversite öğrencilerinin karar verme stilleri, risk alma tercihleri, cinsiyet ve yaş gibi demografik özellikleri ve kişilik özellikleriyle siber güvenlik davranış niyetlerini inceledikleri çalışmada, cinsiyetin siber güvenlik davranışı niyetlerini tahmin edici önemli bir demografik özellik olduğunu belirtmişlerdir. Bu çalışmada, özellikle kadınların güncelleme, güçlü şifre oluşturma ve proaktif farkındalıklarının erkeklere göre daha zayıf düzeyde gösterdikleri bulunmuştur. Bilgisayar becerileri, medya okuryazarlığı ya da çevrimiçi risklerle ilgili yapılan birçok çalışmanın cinsiyete göre sonuçları incelendiğinde aslında genellikle erkeklerin kadınlara oranla öz yeterlik inançları, bilgi ve becerilerinin ya da farkındalık düzeylerinin daha fazla olduğu ortaya çıkmıştır (Dodel ve Mesch, 2018; Eryılmaz, 2018; Scherer ve Siddiq, 2015; Tondeur, Scherer, Siddiq ve Baran, 2017). Bu anlamda erkeklerin dijital araçlarda güvenlik öz yeterlik düzeylerinin kadınlara göre daha yüksek olması diğer çalışmalarla benzerlik göstermektedir. Üniversite öğrencilerinin cinsiyetleri bağlamında, şimdiki çevrimiçi risk alma eğilimi incelendiğinde sosyalleşme riskleri, ticari riskler ve kişisel bilgileri açma riskleri eğilimleri erkeklerde kadınlara oranla daha yüksek, başkalarına zarar verme riskleri ise kadınlarda erkeklere oranla daha yüksek olduğu sonucuna

ulaşılmıştır. Fakat geçmişteki çevrimiçi risk alma eğilimi incelendiğinde katılımcıların tüm risk faktörlerinde erkeklerde kadınlara oranla daha yüksek düzeyde eğilimi olduğu sonucuna ulaşılmıştır. Burada genel olarak gerçek yaşam risklerinin incelendiği çalışmalarda cinsiyet değişkeni incelendiğinde erkeklerin kadınlara göre daha fazla riskli davranışta bulundukları belirlenmiştir (Nicholson, Soane, Fenton-O'Creevy ve Willman, 2005). Bu durum çevrimiçi risklerle ilgili çocuklar üzerinde gerçekleştirilen çalışmalarda da erkek çocukların kadın çocuklara oranla daha fazla çevrimiçi ortamlarda riskli davranış gösterdikleri, bu durumun da çevrimiçi risklerle başa çıkabilme becerilerinin daha yüksek olması da olabilir. Bu çalışmada farklı olarak etki büyüklüğü küçük düzeyde olsa da kadınların başkalarına zarar verme riskleri eğilimi bağlamında şimdiki çevrimiçi risk alma eğiliminin geçmiştekine göre daha yüksek olması oldukça ilginç bir sonuçtur.

Yaş değişkeni bağlamında dijital güvenlik öz yeterlik düzeyleri ele alındığında, dijital uygulamalarda güvenlik düzeylerinde yaş grupları arasında bir farklılığa neden olmazken, üniversite öğrencilerinin dijital araçlarda güvenlik öz yeterlik düzeyleri 22 yaş ve üstü bireylerde 21 yaş ve altı bireylere oranla daha yüksek olduğu ortaya çıkmıştır. Genellikle yetişkin bireyler, çocuk bireylere oranla fayda zarar muhakemesi konusunda gelişimsel olarak daha üst seviyededirler. Fakat yetişkin bireylerin internet kullanım durumları genç bireylere göre kıyaslandığında, genç bireylerin daha fazla sıklıkta ve çeşitlilikte internet teknolojilerini kullandıkları da alanyazında oldukça sıkça karşılaşılan bir sonuçtur. İlgili çalışmada aslında genel olarak genç yetişkinlikte olan bireylerin iki ayrı gruplanması söz konusudur. Bu durumda daha üst yaş grubunda olan üniversite öğrencilerinin daha alt gruptakilere oranla daha fazla çeşitlilikte ve amaçlarda dijital uygulamaları kullandıkları ve hatta en önemlisi bu uygulamalar konusundaki güvenlik deneyimlerini daha fazla kazanmış olmaları muhtemeldir. Üniversite öğrencilerinin yaş grupları bağlamında şimdiki çevrimiçi risk alma eğilimleri incelendiğinde şimdiki sosyalleşme riskleri, kişisel bilgileri açma riskleri ve başkasına zarar verme riskleri bakımından eğilimleri 21 ve altı yaş ve 22 yaş ve üstü yaş gruplarında benzer, şimdiki ticari riskler eğilimleri 21 ve altı yaş grubunda, 22 ve üstü yaş grubuna oranla düşük olduğu sonuçlarına ulaşılmıştır. Bu sonuçlar bağlamında aslında üniversite öğrencilerinin ticari riskler bağlamındaki eğilimlerinin, yaş yükseldikçe arttığı düşünülebilir. Çünkü maddi bir karşılığı olan hizmetin edinilmesi için o kazancı yönetebiliyor olmak gerekmektedir. Söz konusu yaş grupları bağlamında düşünüldüğünde de üniversite

öğrencilerinin ilk yıllarındaki maddi destekleri nasıl harcayacakları konusundaki yönetim becerileri daha sonraki yıllarında değişim gösteriyor olabilir.

Üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri öğrenim gördükleri bilim dallarına göre farklılaşmakta ve fen bilimlerinde öğrenim gören üniversite öğrencilerinin sosyal bilimlerdekilere oranla dijital güvenlik öz yeterlik düzeylerinin yüksek olduğu sonucuna ulaşılmıştır. Şimdiki çevrimiçi risk alma eğilimi açısından elde edilen bulgular doğrultusunda ticari riskler ile başkasına zarar verme riskleri eğilimleri bakımından üniversite öğrencilerinin öğrenim gördükleri bilim dallarına göre bir farklılık olmazken, sosyal bilimlerde öğrenim gören üniversite öğrencilerinin, fen bilimlerinde öğrenim gören üniversite öğrencilerine oranla sosyalleşme riskleri ve kişisel bilgilerini açma riskleri eğilimlerinin daha yüksek olduğu sonuçlarına ulaşılmıştır. Bunun nedeni olarak, sosyal bilimlerde öğrenim gören üniversite öğrencilerinin fayda-zarar muhakeme yeteneklerinin veya karar verme stillerinin, fen bilimlerinde öğrenim gören üniversite öğrencilerinden farklılaşması (Tatlılıoğlu, 2014) ya da çevrimiçi sosyalleşme ve kişisel bilgileri açma riskleri hakkındaki farkındalık düzeylerinin daha düşük olmasından kaynaklanmış olabilir.

İnternet kullanım sıklığı bağlamında üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri ele alındığında, günde 5 saat ve üstü internet kulanım sıklığına sahip üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri günde 3 saat ve altı sıklığında internet kullanan üniversite öğrencilerine göre daha yüksek olduğu sonucuna ulaşılmıştır. Bunun nedeninin internet teknolojilerinin kullanım süresinin artmasıyla karşılaşılacak güvenlik tehditlerinin neler olabileceği konusundaki farkındalık düzeylerinin artması, dijital güvenliğin sağlanması için gerekli olabilecek stratejileri veya becerileri kazanmaları olabilir. Bunun yanında güvenli bir şekilde internet teknolojilerinin kullanımının, o teknolojiler aracılığıyla yaşanılan deneyimlerle ilgilisi olabilir (Kim, Kim, Choi ve Trivedi, 2017). Çünkü, Jeske ve Van Schaik (2017), 18-60 yaş aralığındaki bireylerin katılımcıları olduğu araştırmada, internette geçirilen zaman ve buradaki deneyim sürelerinin uzunluğunun, internet tehditlerine olan aşinalıkları üzerinde önemli bir yordayıcı olduğunu belirtmiştir. Aynı zamanda her iki sıklığın güvenli bilgisayar kullanımını doğrudan olmayan bir tahmin edicisi olduğu da önemli bulguları arasındadır. Benzer şekilde, Kruger, Drevin ve Steyn (2010) sosyal medya, mobil cihazlar ve kablosuz teknolojilerle ilgili güvenli kullanımı daha iyi bir düzeye getirmek için, bu teknolojileri kullanıcılarının, dijital güvenlik tehditleriyle ilgili bilgi eksikliklerinin

üstesinden gelinmesine, internet tehditleri hakkındaki farkındalık düzeylerinin arttırılmasına yardımcı olunması gerektiğini belirtmişlerdir. Dolayısıyla internet kullanım sıklığı arttıkça, dijital uygulamalar veya araçlardaki güvenlik tehditlerinin farkındalığını arttırması ve bu konuda bireylerin dijital güvenlik öz yeterlik düzeylerinin yükselmesi desteklenen bir sonuçtur. Üniversite öğrencilerinin Çevrimiçi Risk Alma Eğilimlerinin internet kullanım sıklığına göre incelenmesi sonucunda elde edilen bulgular doğrultusunda ise şimdiki sosyalleşme riskleri, ticari riskler boyutlarında, günde 5 saat ve üstü sıklığında internet kullanan üniversite öğrencilerinin eğilimlerinin günde 3 saat ve altı ve günde 3-5 saat arası internet kullananlardan yüksek olduğu sonucuna ulaşılmıştır. Şimdiki kişisel bilgileri açma riskleri boyutunda günde 5 saat ve üstü sıklığında internet kullanan üniversite öğrencilerinin günde 3 saat ve altı sıklığında internet kullanan gruptan yüksek olduğu belirlenmiştir. İnternet kullanım sıklığının şimdiki başkasına zarar verme riski boyutu bağlamında ise grupların benzer eğilimler gösterdiği sonucuna ulaşılmıştır.

Üniversite öğrencilerinin dijital uygulamalarda güvenlik öz yeterlik düzeyleri arttıkça şimdiki ticari riskler, geçmişteki ticari riskler ve başkasına zarar verme riskleri eğilimlerinin arttığı sonucuna ulaşılmıştır. Bunun yanında üniversite öğrencilerinin dijital uygulamalarda güvenlik öz yeterlik düzeyleri arttıkça şimdiki başkasına zarar verme riskleri eğilimlerinin azaldığı sonucuna ulaşılmıştır. Üniversite öğrencilerinin dijital araçlarda güvenlik öz yeterlik düzeyleri arttıkça şimdiki sosyalleşme, ticari riskler ve başkasına zarar verme riskleri ve geçmişteki sosyalleşme riskleri ve ticari riskleri eğilimlerinin arttığı sonucuna ulaşılmıştır. Belirtilen sonuçlara bakıldığında dijital araçlarda ve uygulamalarda güvenlik öz yeterliklerinin artmasıyla aslında üniversite öğrencilerinin çeşitli çevrimiçi risk alma eğilimlerinin azalması beklenmektedir. Çünkü Verkijika (2018), çalışmasında mobil araçların güvenliğini sağlama davranışlarını öngörmede bu araçlarda güvenliğin nasıl sağlanması gerektiği bilgi ve becerilerine olan inancın yani öz yeterliğin, önemli bir değişken olduğu belirtilmiştir. Fakat dijital araçlar bağlamında şimdiki ve geçmişteki ticari risk eğilimleri, dijital uygulamalar bağlamında ise şimdiki ve geçmişteki sosyalleşme ve ticari riskler eğilimleri ve geçmişteki başkasına zarar verme risklerinin arttığı görülmektedir. Van Bavel, Rodríguez-Priego, Vila ve Briggs (2019) gerçekleştirdikleri deneysel bir araştırmada, siber güvenliği sağlamak için, internet teknolojileri kullanıcılarına, bir görevi güvenli bir şekilde yerine getirmede ihtiyaç duydukları bilginin sağlanmasının önemli olduğunu, bir siber güvenlik tehditine

karşı önlem alma konusunda "başa çıkma" bilgisi ile desteklenmeleri güvenli davranışların iyileştirilmesinde etkili olduğu bulunmuştur. Van Schaik, Jansen, Onibokun, Camp ve Kusev (2018) ise Facebook kullanıcıları ile gerçekleştiridiği çalışmasında Facebook güvenliği ve genel olarak gizlilikle ilgili korkunun artmasının, algılanan riski arttırdığı ve böylece bu platformdaki güvenli gizlilik ve güvenlik ayarlarını seçmelerini etkilediği sonucuna ulaşılmıştır. Dolayısıyla üniversite öğrencilerinin çevrimiçi risk türlerine göre risk algılarının, bu tehlikelerle karşılaştıklarında dijital güvenlik önlemleri alma davranışlarını arttırdığı ifade edilebilir. Yani bir bakıma üniversite öğrencilerinin risk türlerine göre çevrimiçi risk alma eğilimleri, yeterli dijital güvenlik becerilerine sahip olduklarından bu ilişkileri göstermiş olabilirler. Üniversite öğrencilerinin dijital araçlardaki güvenlik öz yeterlikleri ile şimdiki ve geçmişteki sosyalleşme risklerinin ilişkisi dijital uygulamalarda güvenlik öz yeterlik düzeyleri ile şimdiki ya da geçmişteki sosyalleşme riskleri arasında bir sonuç bulunmaması da oldukça önemli bir sonuçtur. Çünkü sosyal medya, sohbet odaları veya çevrimiçi ilgi grupları gibi dijital uygulamalarda gerçekleştirilebilecek etkinliklerde internet ve uygulamalar aracılığıyla sağlanan iletişim, etkileşim ve veri alışverişi söz konusudur. Başkalarına zarar verme riskleri ise çalışma kapsamında siber zorbalıkla ilgili olabilecek ayrıntılı olmayan çevrimiçi davranışları kapsamaktadır. Gratian, Bandi, Cukier, Dykstra ve Ginther (2018) ise bireylerin gerçek yaşamda risk alma tercihleri ile siber güvenlik davranışı niyetleri ile ilişkili olmadığı bulgusuna ulaşmıştır. Dolayısıyla yetişkinlerin bu davranışlarının gelişim dönemleri veya sosyal istenirlik düzeyleriyle ilişkili olarak değişim gösterdiği düşünülebilir. Üniversite öğrencilerinin şimdiki ve geçmişteki çevrimiçi risk alma eğilimi incelendiğinde geçmişteki çevrimiçi risk alma eğilimleri arttıkça şimdiki Çevrimiçi Risk Alma Eğilimlerinin de artığı sonucu elde edilmiştir. Bu sonuç aslında bireylerin geçmişteki davranış sıklıklarının şimdiki davranış sıklıkları ile ilişkisinin olduğu sonucunu vurgulamaktadır.

Üniversite öğrencilerinin sırasıyla geçmişteki ticari riskler, kişisel bilgileri açma riskleri, başkasına zarar verme riskleri ve sosyalleşme riskleri eğilimleri en çok tahmin edenden en az tahmin edene doğru şimdiki çevrimiçi risk alma eğilimlerini yordadığı sonucuna ulaşılmıştır. Ben-Asher ve Gonzalez (2015), bilişim sistemlerinin güvenliği sağlamak için bireylerin kararlarının oldukça farkındalığı artmaktadır. Özellikle, geçmiş deneyimlerin ve bilginin siber dünya gibi son derece dinamik bir ortamda karar vermeyi nasıl etkilediğini anlamanın önemini vurgulamıştır. Van Schaik, Jeske, Onibokun,

Coventry, Jansen ve Kusev (2017), siber ortamlarda riskli davranışlarda bulunmanın, risk alma eğilimi ve risk algısı tarafından etkilendiğini belirterek, çalışmasının sonucunda olumsuz sonuçlara yol açabilecek kedi avcılığı gibi çevrimiçi sosyalleşme tehlikelerinin üniversite öğrenciler tarafından daha az riskli olarak algılandığını belirmiştir. Ayrıca listeledikleri 16 internet tehlikesinin bireysel sonuçlarının ciddiyeti ne kadar yüksekse algılanan riskin de o kadar yüksek olduğu ve her tehdite göre bu risk algısının değiştiği sonuçlarına ulaşılmıştır. Dolayısıyla geçmişteki üniversite öğrencilerinin ticari riskler ve kişisel bilgileri açma risklerini diğer risk türlerine göre daha ciddi sonuçlar yaratacağını düşünmeleri risk algılarını arttırabileceğinden, sırasıyla geçmişteki ticari riskler, kişisel bilgileri açma riskleri, başkasına zarar verme riskleri ve sosyalleşme riskleri eğilimleri en çok tahmin edenden en az tahmin edene doğru şimdiki çevrimiçi risk alma eğilimlerini yordamış olabilir. Bu sıralamanın nedeni bir diğer yönden, bireylerin yetişkinlik düzeyleri arttıkça e-ticaret e-alışveriş gibi finansal işlemlerini internet teknolojileri aracılığıyla yönetmesi, ekonomik özgürlüklerini kazandıkça ve çeşitli e-ticaret veya e-bankacılık gibi hizmetler çeşitlendikçe kullanıcıların bu tür hizmetleri daha çok kullanacağı ve dolayısıyla kullanım sıklıklarının çeşitli çevrimiçi risk alma eğilimlerini arttırabileceği olarak yorumlanabilir. Geçmişteki sosyalleşme nedenleri de aslında geçmişteki ticari riskler eğilimlerinin nedenlerinde olduğu gibi bireylerin giderek değişen ihtiyaçları doğrultusunda şekillenebilir.

Dijital güvenlik öz yeterliği, dijital güvenlik becerileri dolayısıyla güvenli internet kullanımı açısından oldukça önemli bir konudur. Son zamanlarda, medya okuryazarlığı, dijital okuryazarlık, 21. yy. becerileri, bilgisayar kullanma becerileri kapsamında sıklıkla ele alınan dijital güvenlik konusu, daha önceki yıllarda sadece araçsal yani kullanılan teknolojik araçtaki güvenlik olarak algılanırken, değişen ve gelişen web teknolojileri, internetin artan oran ve sıklıkta kullanılmasıyla sadece dijital aracın değil de çevrimiçi dünyayla ilgili kullanılan her araç, uygulama veya altyapı (ağ bağlantısı vb.) da güvenliğin oldukça önemli olduğu ve sağlanması için dijital teknoloji kullanıcılarının sahip olması gereken birtakım bilgi ve becerilerin olması gerçeği ortaya çıkmıştır. Dijital güvenlikle ilgili değişkenler incelendiğinde, internete bağlanan araçlar veya çevrimiçi hesaplarda güçlü şifre oluşturma, güvenli ağ bağlantılarını kullanma, kullanıcı verilerinin korunması, sosyal ağlardaki gizlilik ve güvenliği sağlama gibi web uygulamalarında gizlilik ve güvenliğin sağlanması başlıklarının birleşimini kapsayan bir konu olduğu görülmüştür. Çalışma kapsamında geliştirilen dijital güvenlik öz yeterlik ölçeği dijital

araçlarda ve dijital uygulamalarda güvenlik öz yeterliği faktörlerine ayrılmıştır. Bu durum aslında dijital güvenliğin sadece virüs programı ya da güvenlik duvarı kullanma, verileri yedekleme veya şifreleme gibi dijital araçlarda değil, aynı zamanda medya okuryazarlığı, dijital okuryazarlık kapsamında değerlendirilebilecek kişilerin çevrimiçi uygulamalarda güvenlik ayarlarını yapılandırabilmesi, e-bankacılık veya e-ticaret işlemlerinde güvenilir yöntemler kullanabilmesi gibi dijital uygulamalarda da güvenliğin sağlanması gerektiğini kanıtlamıştır.

Çevrimiçi riskler ise özellikle 9-18 yaş aralığındaki çocuk bireylerin interneti kullanım oranının artması, çeşitli çevrimiçi oyunlar, sanal dünyalar veya sosyal ağlarda oldukça fazla vakit geçirmeleri ve bu ortamlar aracılığıyla kendilerinin fiziksel, duyuşsal ya da psikolojik olarak dijital teknolojiler vasıtasıyla iyi oluşlarını olumsuz yönde etkileyen zararları gelişimsel olarak mantık süzgecinden geçirememeleri, yarar-zarar dengesini kuramamaları ve bazı risklerle baş edebilecek stratejileri bilmemeleri sebebiyle birçok araştırma tarafından ele alınan bir konu olmuştur. Bu tür çalışmalarda çocukların karşılaştıkları siber zorbalık, kandırılarak kişisel bilgilerinin elde edilmesi gibi çevrimiçi riskli davranışlarla ne kadar karşılaştıkları veya bu davranışları ne kadar gösterdikleri ele alınmıştır. Ayrıca bu çalışmalarda çeşitli çevrimiçi riskler çerçeveleri de oluşturulmuştur. Son zamanlarda medya araştırmaları ya da sınırlı sayıdaki bilimsel araştırmalarda ise çevrimiçi riskli davranışlar konusunun yetişkin bireyler açısından da ele alınması gerektiği, yetişkinlerin internet teknolojilerinin önemli oranda kullanıcısı oldukları ve interneti kullanım amaçlarının çocuklardan farklılaşması, karşılaşabilecekleri veya davranışta bulunabilecekleri çevrimiçi riskleri de farklılaştırmıştır. Dolayısıyla son zamanlarda yetişkinlerin de ele alındığı çevrimiçi risklerle ilgili araştırmalarda finansal riskler, sosyalleşme riskleri gibi çevrimiçi risklerle karşılaştıkları veya bu riskli davranışları gösterdikleri çevrimiçi riskler çerçeveleri oluşturulmuştur. Bu çalışmada çevrimiçi risk alma eğilimi ölçeği kapsamında üniversitede öğrenim gören genç yetişkinlerin gösterdikleri çevrimiçi riskli davranışlar çerçevesi sosyalleşme riskleri, ticari riskler, kişisel bilgileri açma riskleri ve başkalarına zarar verme risklerinden oluşmuştur.

Hem dijital güvenlik hem de çevrimiçi riskler konuları oldukça dinamik yapılara sahiptirler. Çünkü geliştirilen her yazılım veya uygulamanın güvenlik açığı, yeni çıkan virüsler, şifre edinen uygulamalar, gerçek dünyada olduğu gibi her sosyal ağda niyetinin ne olduğu bilinmeyen kullanıcıların edindikleri bilgiler doğrultusunda yapabileceklerinin

çeşitlenmesi, kişilerin verilerinin kötü amaçlı kullanımı, sanal cinsel sosyalleşme, şiddet, ayrımcılık, düşmanlık ve yanlış bilgi içeren uygunsuz içeriklerin sürekli olarak üretilmesi, ulaşılabilecek para karşılığı yapılan e-hizmetlerde dolandırıcılık gibi tüm tehditlerin her geçen gün yenileri ortaya çıkmaktadır. Dolayısıyla bu araştırmaya ilgili alanyazın doğrultusunda, genç yetişkinlerin çevrimiçi risk alma eğilimleri ve dijital güvenlik öz yeterlikleri arasında anlamlı ilişkilerin olduğu varsayımı ile yola çıkılmıştır. Temel alınan bu değişkenler bireylerin cinsiyet, yaş, öğrenim gördükleri bilim dalları internet kullanım sıklıkları gibi birçok bağımsız değişken tarafından da incelenmiştir. Bilgisayar güvenliği, medya okuryazarlığı, 21. yy. becerileri gibi birçok araştırmada cinsiyet, yaş, internet kullanım sıklığı gibi değişkenlerin bireylerin öz yeterlikleri, tutum veya davranışlarını etkileyebileceği ortaya konulmuştur.

4.3. Öneriler

Bu bölümde çalışmanın sonuçları doğrultusunda, eğitim kurumları, sivil toplum kuruluşları, araştırmacılar ve eğitmenler için uygulamaya ve araştırmaya yönelik çeşitli önerilerde bulunulmuştur.

4.3.1. Uygulamaya yönelik öneriler

- Genel olarak internet teknolojilerini kullanan genç yetişkinlerin dijital araçlarda güvenlik öz yeterlikleri, dijital uygulamalarda güvenlik öz yeterlik düzeylerinden daha yüksek çıkmıştır. Bu doğrultuda özellikle dijital uygulamalarda kullanıcıların hangi güvenlik önlemlerini alabileceği, bu önlemleri almadığında hangi çevrimiçi risklerle karşılaşabilecekleri konusunda farkındalıklarını arttıracak eğitsel faaliyetler düzenlenmeli, etkililiği değerlendirilmeli ve belirli aralıklarla bu eğitimler güncellenmelidir.
- Dijital uygulamalarda güvenlik öz yeterliği kapsamında kadın üniversite öğrencilerinin düzeyleri erkek üniversite öğrencilere göre düşük çıkması sonucu doğrultusunda, özellikle kadın bireylerin dijital güvenlik öz yeterlik düzeylerini arttırıcı, uygulamalı çeşitli dijital tehditlerle nasıl başa çıkabilecekleri konusunda eğitimler düzenlenmeli ve bu eğitimlerin etkililiği değerlendirilmelidir.

- Üniversite öğrencilerinin ilk yıllarında ihtiyaç duydukları sosyalleşme, grup oluşturma, başkalarıyla iletişim ve etkileşim kurma ihtiyaçlarını, özellikle sosyalleşme ve kişisel bilgilerini ifşa etme gibi riskleri almadan önce kimlerle, ne zaman ve nasıl kullanılacağını öngöremediği bilgi paylaşımında bulunmamaları için, bilgi ve iletişim teknolojilerinin güvenli kullanımı konusunda hazırlık eğitimi almaları sağlanmalıdır.
- Yaş grubu büyük olan üniversite öğrencilerinin ticari riskler eğilimlerinin küçük yaştakilere oranla yüksek olduğu sonucuna yönelik özellikle yetişkinlerin günümüzde sanal ortamlar aracılığıyla dolandırıldıkları örneklerinin de artmasıyla, yaşanılan örnek olaylar benzeri deney ortamları aracılığıyla, gerçek maddi zarara sebebiyet vermeyen fakat gerçekçi deneyim kazandıran uygulamalar gerçekleştirilebilir.
- Üniversite öğrencilerinin geçmişteki kişisel bilgileri açma riskleri bağlamında düşük yaş grubundaki bireylerin eğilimlerinin büyük yaş grubundakilere oranla daha fazla olduğu sonucu elde edilmiştir. Bireylerin internet teknolojilerini kullanmaya başlama yaşları dikkate alınarak veya günümüzde en çok kullandıkları Facebook, Instagram, çevrimiçi çok kullanıcılı oyunlar vb. başka kişilerle paylaşımda veya bilgi, dosya alışverişinde bulunduğu platformlarda hangi bilgilerinin paylaşılmasının hassas olduğu ve ileride sebep olabilecek kimlik hırsızlığı gibi tehditlere karşı neler yapılabileceği konusunda bilgilendirici farkındalık çalışmaları düzenlenebilir.
- Sosyal bilimler bilim dalında öğrenim gören üniversite öğrencilerinin sosyalleşme ve kişisel bilgileri açma riskleri eğilimlerinin fen bilimlerindekilere oranla yüksek olması doğrultusunda, sosyal bilimlerde öğrenim gören üniversite öğrencileri için çevrimiçi davranışlarda yapılabilecek fayda-zarar muhakemelerinin gelişmesi ve analitik düşünme becerilerini tetikleyici etkinlikler düzenlenebilir.
- Genel olarak dijital güvenlik öz yeterlik düzeyi ve çevrimiçi risk alma eğilimi açısından üniversite öğrencilerinin, internet kullanım sıklıkları arttıkça hem dijital güvenlik öz yeterlik düzeyleri hem de çevrimiçi risk alma eğilimleri arttığı sonucu doğrultusunda, aslında katılımcıların güvenli internet kullanım deneyimlerini arttırıcı, bilgilendirici ve uygulamaya

yönelik çalışmalar yürütülebilir ve bireylerin bu süreçte güvenli bir şekilde internet teknolojilerini kullanabilmeleri için işe koştukları stratejiler örnek olaylarla birlikte açıklanabilir.

4.3.2. Araştırmaya yönelik öneriler

- Alanyazında da sıklıkla belirtilen internet tehditlerinin her geçen gün yenilenmesi doğrultusunda güvenli internet teknolojilerinin kullanımı için yeni bilgi ve becerilerin kazanılması gerekebilir. Bu doğrultuda dijital güvenlik öz yeterlik ölçeği söz konusu tehditler ve bu tehditler karşısında alınabilecek önlemler çerçevesinde güncellenebilir.
- Çevrimiçi riskler çerçevesi gelişen her internet teknolojisi kapsamında karşılaşılabilecek risk türleri değişebilir. Bu doğrultuda geliştirilen çevrimiçi risk alma eğilimi ölçeği yenileri eklenen risk türlerine göre güncellenebilir.
- Çevrimiçi riskler çerçeveleri internet kullanıcılarının gelişim dönemlerine göre farklı davranışları içermektedir. Bu nedenle üniversite öğrencileri üzerinde geliştirilen çevrimiçi risk alma eğilimi ölçeği çocuklarda veya üniversite öğrencilerinden daha yetişkin düzeyde olan bireyler üzerinde denenip, çevrimiçi risk alma eğilimi yapısı tekrar incelenebilir.
- Çalışma kapsamında üniversite öğrencileri düzeyinde geliştirilen her iki ölçme aracı, 9-18 yaş aralığında yer alan çocuk katılımcılar üzerinde de madde havuzu kullanılarak geçerlik ve güvenirlik çalışmaları tekrarlanabilir.
- Çevrimiçi risk alma eğilimi bakımından genel olarak cinsiyete göre sonuçlar ele alındığında erkek üniversite öğrencilerinin kadınlara göre daha fazla sıklıkta çevrimiçi riskli davranışlarda bulunduğu ortaya çıkmıştır. Bu bağlamda erkek bireylerin neden daha sık bu davranışları gösterdiklerini ortaya koyacak nitel araştırma desenlerinin ve veri toplama türlerinin kullanıldığı araştırmalar yürütülebilir.
- Küçük yaş ve büyük yaş grubundaki bireylerin kişisel bilgilerini çeşitli sanal platformlarda veya gruplarda neden paylaştıklarını ortaya koyacak ve bu yaş gruplarını karşılaştıracak araştırmalar yürütülebilir.

- Genel olarak üniversite öğrencilerinin internet kullanım sıklıkları ne kadar fazlaysa o oranda dijital güvenlik öz yeterlik düzeyleri ve çevrimiçi risk alma eğilimleri artmaktadır. Umulanın aksine olan bu sonuç doğrultusunda, öğrencilere çeşitli çevrimiçi riskler karşısında gerçekte hangi dijital güvenlik becerilerini işe koştuklarını ve bu konuda kendilerine olan öz yeterliklerinin gerçek davranışları yordama durumları ele alınabilir.
- Üniversite öğrencilerinin dijital güvenlik öz yeterlik düzeyleri arttıkça genel olarak çevrimiçi risk alma eğilimleri arttığı belirlenmiştir. Bu doğrultuda çevrimiçi risk alma eğilimi, risk algısı, çevrimiçi risklerle başa çıkma stratejileri, kişilik özellikleri gibi, gerçek yaşam risklerinin alınmasında etkili olan değişkenler ile ilişkili olan değişkenler ile de incelenebilir.
- Genç yetişkinlerin geçmişlerindeki ticari riskler konusundaki eğilimlerinin şimdiki çevrimiçi risk alma eğilimlerini oldukça yüksek düzeyde yordadığından, e-bankacılık, e-hizmetler, e-alışveriş vb. finansal bilgi paylaşımı gerektiren işlemlerde sahip olmaları ve bilmeleri gereken dijital güvenlik becerileri konusunda eğitimler düzenlenmeli ve bu eğitimlerin etkililiği dijital güvenlik becerileri, medya okuryazarlıkları, risklerle başa çıkma stratejileri ve kişilik özellikleri gibi çeşitli değişkenlerle incelenebilir.
- Üniversite öğrencilerinin çevrimiçi risk alma eğilimi sırasıyla geçmişteki ticari riskler, kişisel bilgilerini açma, başkasına zarar verme ve sosyalleşme riskleri eğilimleri tarafından yordanması, aslında bu risk faktörlerinin hangisini daha riskli olarak algıladıklarından da kaynaklanabileceğinden, devam eden araştırmalarda çevrimiçi risk algısı değişkeninin çevrimiçi risk alma eğilimini nasıl etkilediği ortaya konulabilir.

KAYNAKÇA

Agosto, D. E. and Abbas, J. (2017). "Don't be dumb—that's the rule I try to live by": A closer look at older teens' online privacy and safety attitudes. *New Media & Society,* 19 (3), 347-365.

Akbulut, Y. (2010). *Sosyal bilimlerde SPSS uygulamaları: Sık kullanılan istatistiksel analizler ve açıklamalı SPSS çözümleri*. İstanbul: İdeal Kültür Yayıncılık.

Akcil, U., Altinay, Z. and Altinay, F. (2016). Assessing the effects of managers in the digital age on the management process of digital citizenship roles. *The Anthropologist,* 23 (1-2), 209-217.

Arslan, H. (2014). Eleştirel medya okuryazarlığı kapsamında çocuk odaklı haber ve programlar üzerine bir değerlendirme. *Sosyal Bilimler Enstitüsü Dergisi,* 1 (2), 71-79.

Baker, D.B. (2015). Trustworthy systems for safe and private healthcare. In: Saba, V., McCormick, K. (Eds.), in *Essentials of nursing informatics* (6th edition, Chapter 10). McGraw- Hill Education, ISBN-978-0-07-182955-7.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psycholist,* 37 (2), 122-147.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall, Englewood Cliffs, NJ.

Baştürk Akça, E., Sayımer, İ. ve Ergül, S. (2015). Ortaokul öğrencilerinin sosyal medya kullanımları ve siber zorbalık deneyimleri: Ankara örneği. *Global Media Journal: Turkish Edition,* 5 (10).

Baumgartner, S. E., Valkenburg, P. M. and Peter, J. (2010). Unwanted online sexual solicitation and risky sexual online behavior across the lifespan. *Journal of Applied Developmental Psychology,* 31 (6), 439-447.

Ben-Asher, N. and Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior,* 48, 51-61.

Browne, M. W. and Cudeck, R. (1992). Alternative ways of assessing model fit. *Sociological Methods & Research,* 21 (2), 230-258.

Byrne, Z. S., Dvorak, K. J., Peters, J. M., Ray, I., Howe, A. and Sanchez, D. (2016). From the user's perspective: Perceptions of risk relative to benefit associated with using the Internet. *Computers in Human Behavior,* 59, 456-468.

Calvani, A., Fini, A., Ranieri, M. and Picci, P. (2012). Are young generations in secondary school digitally competent? A study on Italian teenagers. *Computers & Education,* 58, 797-807.

Cansever, B. A. (2015). Where are computer and internet in a child's life? *International Journal of New Trends in Arts, Sports ve Science Education (IJTASE),* 3 (4).

Ceyhan, E. B., Demiryürek, E. ve Kandemir, B. (2015). Sosyal ağlarda güncel güvenlik riskleri ve korunma yöntemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* 1 (1).

Chang, F. C., Miao, N. F., Chiu, C. H., Chen, P. H., Lee, C. M., Chiang, J. T. and Chuang, H. Y. (2016). Urban–rural differences in parental Internet mediation and adolescents' Internet risks in Taiwan. *Health, Risk & Society,* 18 (3-4), 188-204.

Chauhan, S. and Panda, N. K. (2015). Online security. *In hacking web ıntelligence: open source intelligence and web reconnaissance concepts and techniques.* (p. 203-216). Syngress. https://doi.org/10.1016/B978-0-12-801867-5.00011-2

Christofides, E., Muise, A. and Desmarais, S. (2010). The effect of personality factors in predicting information disclosure online. *In Poster presented at the 2010 conference of the Society for Personality and Social Psychology,* Las Vegas, NV.

Cohen, J. (1988). *Statistical power analysis fort he behavioral sciences* (2nd edition). Hillsdale, NJ: Erlbaum.

Comrey, A.L. and Lee, H. B. (1992). *A first course in factor analysis* (2nd edition). Hillsdale, NJ: Erlbaum.

Cresswell, J. (2012) *Educational research: Planning, conducting and evaluating quantitative and qualitative research* (4th edition). Pearson: Boston.

Çelik, E. H. ve Yılmaz, V. (2013). *LISREL 9.1 ile yapısal eşitlik modellemesi: Temel kavramlar, uygulamalar, programlama*. Ankara: Anı Yayıncılık.

Çokluk, Ö., Şekercioğlu, G. ve Büyüköztürk, Ş. (2012). *Sosyal bilimler için çok değişkenli istatistik: SPSS ve LISREL uygulamaları* (2. baskı). Ankara: Pegem A Yayıncılık.

Çokluk, Ö., Şekercioğlu, G. ve Büyüköztürk, Ş. (2014). *Sosyal bilimler için çok değişkenli istatistik SPSS ve Lisrel Uygulamaları* (3. baskı). PegemAkademi: Ankara.

De Bruijn, H. and Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly,* 34 (1), 1-7.

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L. and Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics,* 35 (5), 1277-1287.

Demirel, M., Yörük, M. ve Özkan, O. (2013). Çocuklar için güvenli internet: Güvenli internet hizmeti ve ebeveyn görüşleri üzerine bir araştırma. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 4 (7), 54-68.

DeVellis, R.F., (2012). *Scale Development: Theory and applications* (3rd edition). Sage Publications, California.

Doane, A. N., Boothe, L. G., Pearson, M. R. and Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computers in Human Behavior,* 60, 508-513.

Dodel, M. and Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society,* 21 (5), 712-728.

Dönmez, O. ve Akbulut, Y. (2016). Siber zorbalık çalışmalarında sosyal beğenirlik etmeni. *Eğitim Teknolojisi Kuram ve Uygulama,* 6 (2), 1-18.

Erol, O., Şahin, Y. L., Yılmaz, E. and Haseski, H. İ. (2015). Personal Cyber Security Provision Scale development study. *International Journal of Human Sciences,* 12 (2), 75-91.

Eryılmaz, S. (2018). Öğrencilerin bilgi ve iletişim teknolojileri yeterliliklerinin belirlenmesi: Gazi Üniversitesi, Turizm Fakültesi örneği. *Elektronik Sosyal Bilimler Dergisi,* 17 (65), 37-49.

Fan, X., Thompson, B. and Wang, L. (1999). Effects of sample size, estimation methods, and model specification on structural equation modeling fit indexes. *Structural Equation Modeling: A Multidisciplinary Journal,* 6 (1), 56-83, DOI: 10.1080/10705519909540119.

Field, A. (2009). *Discovering statistics using SPSS for Windows* (3rd edition). London: Sage.

Floyd, F. J. and Widaman, K.F. (1995). Factor analysis in the development and refinement of clinical assessment instruments. *Psychological Assessment.* 7 (3), 286-299.

Fornell, C. and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39-50.

Gámez-Guadix, M., De Santisteban, P. and Alcazar, M. Á. (2017). The construction and psychometric properties of the questionnaire for online sexual solicitation and interaction of minors with adults. *Sexual Abuse,* 1079063217724766.

Garg, V. and Camp, J. (2012, January). End user perception of online risk under uncertainty. In 45th Hawaii International Conference on System Sciences (pp. 3278-3287). IEEE.

George, D. and Mallery, P. (2003). *SPSS for Windows step by step: A simple guide and reference. 11.0 update* (4th edition). Boston: Allyn & Bacon.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, 345-358.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon,* 3 (7), e00346.

Hair Jr, J. F., Hult, G. T. M., Ringle, C. and Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd edition). Sage Publications.

Hair, J. F., Black, W. C., Babin, B. J. and Anderson, R. E. (2009). *Multivariate data analysis* (7th edition). Pearson Prentice Hall.

Halamka, J.D. (2017). Chapter 6- Privacy and Security. Sheikh, A., Bates, D. W., Wright, A., and Cresswell, K. (Eds.). (2017). In *Key advances in clinical informatics: Transforming health care through health ınformation technology* (pp. 79-86). Academic Press. https://doi.org/10.1016/B978-0-12-809523-2.00006-6

Hasebrink, U., Livingstone, S., Haddon, L. and Ólafsson, K. (2009). Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online, Deliverable D3. 2. LSE, London, EU Kids Online, http://eprints. lse. ac. uk/24368/1 D, 3.

Henson, R. K. and Roberts, J. K. (2006). Use of exploratory factor analysis in published research common errors and some comment on improved practice. *Educational and Psychological Measurement,* 66 (3), 393-416.

Holloway, D., Green, L. and Livingstone, S. (2013). *Zero to eight. Young children and their internet use*. London: EU Kids Online, LSE.

Hoyle, R.H. (1995). *Structural equation modeling: Concepts, issues, and applications*. London: Sage Publications.

Hu, L. T. and Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, 6 (1), 1-55.

Huang, D. L., Rau, P. L. P. and Salvendy, G. (2007, July). A survey of factors influencing people's perception of information security. In *International Conference on Human-Computer Interaction* (p. 906-915). Berlin, Heidelberg: Springer.

Huang, D. L., Rau, P. L. P. and Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, 29 (3), 221-232.

Huck, S. W. (2012). *Reading statistics and research* (6th edition). Boston: Pearson.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31 (1), 83-95.

Işık, İ. (2014). Yokluk hipotezi anlamlılık testi ve etki büyüklüğü tartışmalarının psikoloji araştırmalarına yansımaları. *Eleştirel Psikoloji Bülteni,* 5, 55-80.

Jalali, M. S., Kaiser, J. P., Siegel, M. and Madnick, S. (2019). The Internet of Things promises new benefits and risks: a systematic analysis of adoption dynamics of IoT products. *IEEE Security & Privacy*, 17 (2), 39-48.

Jeske, D. and Van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security,* 66, 129-141.

Jiang, M., Tsai, H. Y. S., Cotten, S. R., Rifon, N. J., LaRose, R. and Alhabash, S. (2016). Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology,* 42 (9), 621-634.

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

Karasar, N. (2009). *Bilimsel Araştırma Yöntemlerinde Kavramlar, İlkeler, Teknikler* (19. baskı) Ankara: Nobel Yayın Dağıtım.

Kelloway, EK. (1998). *Assessing model fit. Using Lisrel for structural equation modeling* (3rd edition, p. 23-40) USA: Sage Publications. Aktaran Erkorkmaz, Ü., Etikan, İ., Demir, O., Özdamar, K., ve Sanisoğlu, S. Y. (2013). Confirmatory factor analysis and fit indices. *Türkiye Klinikleri Journal of Medical Sciences*, 33 (1), 210.

Kim, M., Kim, J., Choi, J. and Trivedi, M. (2017). Mobile shopping through applications: understanding application possession and mobile purchase. *Journal of Interactive Marketing,* 39, 55-68.

Kline, R. B. (2005). *Principals and practice of structural equation modeling* (2nd edition). New York: The Guilford Press.

Kline, R. B. (2015). *Principals and practice of structural equation modeling* (5th edition). New York: The Guilford Press.

Kruger, H., Drevin, L. and Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security,* 18 (5), 316-327.

Kuoppamäki, S. M., Taipale, S. and Wilska, T. A. (2017). The use of mobile technology for online shopping and entertainment among older adults in Finland. *Telematics and Informatics,* 34 (4), 110-117.

Lau, W. W. and Yuen, A. H. (2016). The relative importance of paternal and maternal parenting as predictors of adolescents' home Internet use and usage. *Computers & Education*, 102, 224-233.

Livingstone, S. and Haddon, L. (2008). Risky experiences for children online: Charting European research on children and the internet. *Children & Society,* 22 (4), 314-323.

Livingstone, S., Haddon, L., Görzig, A. and Ólafsson, K. (2011). Risks and safety on the internet. *The perspective of European children. Full findings and policy implications from the EU Kids Online survey of European children,* 9-16.

Lobe, B., Livingstone, S., Ólafsson, K. and Vodeb, H. (2011). *Cross-national comparison of risks and safety on the internet: Initial analysis from the EU Kids Online survey of European children,* London: EU Kids Online, LSE.

Lomax, R. G. and Schumacker, R. E. (2010). *A beginner's guide to structural equation modeling* (3rd edition). New York, NY: Routledge Academic.

Microsoft (2018). Digital Civility Study. https://news.microsoft.com/apac/2018/02/06/microsoft-digital-civility-study-shows-online-abuse-often-comes-peoples-social-circles/#_ftn1 (Retrieved on: 12.05.2019).

Nicholson, N., Soane, E., Fenton-O'Creevy, M. and Willman, P. (2005). Personality and domain-specific risk taking. *Journal of Risk Research,* 8 (2), 157-176.

Norberg, P. A., Horne, D. R. and Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs,* 41 (1), 100-126.

Nunnally, J. C. and Bernstein, I. H. (1994). *Psychometric theory (McGraw-Hill series in psychology)* (3rd Edition). New York: McGraw-Hill.

OECD, (2012). The Protection of children online. Report on risks faced by children online and policies to protect them. http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf (Retrieved on: 12.12.2015).

Ofcom, (2017). Adult's media use and attidudes. https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes (Retrieved on: 19.06.2018).

Pajares, F. (2002), "Overview of social cognitive theory and of self-efficacy", http://www.uky.edu/~eushe2/Pajares/eff.html (Erişim tarihi: 15.05.2019).

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

Pujazon-Zazik, M. A., Manasse, S. M. and Orrell-Valente, J. K. (2012). Adolescents' self-presentation on a teen dating web site: a risk-content analysis, *Journal of Adolescent Health,* 50 (5), 517-520.

Radyo ve Televisyon Üst Kurulu, (2013). Türkiye'de çocukların medya kullanma alışkanlıkları araştırması, Bizim Matbaa, İstanbul. http://www.byegm.gov.tr/uploads/docs/RTU%CC%88K%EF%80%A2_Tu%CC%88rkiyede_C%CC%A7ocu_klar%C4%B1n_Medya_Kullanm_a_Al%C4%B1s%CC%A7kanl%C4%B1g%CC%86%C4%B1_Aras%CC%A7t%C4%B1_rmas%C4%B1_Eylu%CC%88l_2013.pdf (Erişim tarihi: 15.12.2015).

Radyo ve Televisyon Üst Kurulu, (2016). Medya okuryazarlığı araştırması. https://www.rtuk.gov.tr/rtuk-kamuoyu-arastirmalari/3890/5247/medya-okuryazarligi-arastirmasi-2016.html (Erişim tarihi: 12.05.2019).

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S. and Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, 421, 43-69.

Ribble, M. S., Bailey, G. D. and Ross, T. W. (2004). Digital citizenship: Addressing

appropriate technology behavior. *Learning & Leading with technology*, 32 (1), 6.

Ribble, M. and Bailey, G. (2004). Digital citizenship: Focus questions for implementation. *Learning and Leading with Technology*, 32 (2), 12-15.

Sakarya, S., Tercan, İ. ve Çoklar, A.N., (2012). İlköğretim öğrencilerinin interneti ve arama motorlarını kullanım durumları. *E-Journal of New World Sciences Academy, 1C0500,* 7 (1), 348-354.

Scherer, R. and Siddiq, F. (2015). Revisiting teachers' computer self-efficacy: A differentiated view on gender differences. *Computers in Human Behavior,* 53, 48-57).

Schermelleh-Engel, K., Moosbrugger, H. and Müller, 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.

Schreiber, J.B., Nora, A., Stage, F. K., Barlow, E. A. and King, J. (2006) Reporting structural equation modeling and confirmatory factor analysis results: A Review, *The Journal of Educational Research,* 99 (6), 323-338, DOI: 10.3200/ JOER.99.6.323-338

Šimandl, V. and Vaníček, J. (2017). Influences on ICT teachers knowledge and routines in a technical e-safety context. *Telematics and Informatics,* 34 (8), 1488-1502.

Sitkin, S. B. and Pablo, A. L. (1992). Reconceptualizing the determinants of risk behavior. *Academy of Management Review,* 17 (1), 9-38.

Sitkin, S. B. and Weingart, L. R. (1995). Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. *Academy of Management Journal,* 38 (6), 1573-1592.

Soldatova, G. and Zotova, E. (2013). Coping with online risks: The experience of Russian schoolchildren. *Journal of Children and Media,* 7 (1), 44-59.

Sonck, N., Livingstone, S., Kuiper, E. and De Haan, J. (2011). *Digital literacy and safety skills. EU Kids Online,* London, UK: London School of Economics & Political Science.

Sun, J. C. Y., Yu, S. J., Lin, S. S. and Tseng, S. S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior,* 59, 249-257.

Sütütemiz, N. (2005). *Müşteri sadakati belirleyicileri ve modellerin karşılaştırılması: Bankacılık ve sağlık sektöründe bir araştırma*. Yayımlanmamış doktora tezi, Sakarya Üniversitesi, Sosyal Bilimler Enstitüsü.

Tabachnick, B. G. and Fidell, L. S. (2001). *Using multivariate statistics* (4th edition). MA: Allyn & Bacon, Inc.

Tabachnick, B. G. and Fidell, L. S. (2007). *Using multivariate statistics* (5th edition). New Jersey: Pearson.

Tabachnick, B. G. and Fidell, L. S. (2012). *Using multivariate statistics* (6th edition). New Jersey: Pearson.

Tatlılıoğlu, K. (2014). Üniversite öğrencilerinin karar vermede öz-saygı düzeyleri ile karar verme stilleri arasındaki ilişkinin bazı değişkenlere göre incelenmesi. *Akademik Sosyal Araştırmalar Dergisi,* 1 (2), 150-170.

Thompson, N., McGill, T. J. and Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, 70, 376-391.

Tokel, S. T., Başer, D. ve İşler, V. (2013). Türkiye'deki ebeveynlerin çocuklarının internet ve sosyal paylaşım siteleri kullanımına yönelik bilgi seviyeleri ve algıları. *Mersin Üniversitesi Eğitim Fakültesi Dergisi,* 9 (1), 225-236.

Tondeur, J., Scherer, R., Siddiq, F. and Baran, E. (2017). A comprehensive investigation of TPACK within pre-service teachers' ICT profiles: Mind the gap. *Australasian Journal of Educational Technology,* 33 (3), 46-60.

Türkiye İstatistik Kurumu, (2017). Bilgi toplumu istatistikleri 2004-2017. http://www.tuik.gov.tr/UstMenu.do?metod=temelist (Erişim tarihi: 20.04.2018)

Ullman, J. B. and Bentler, P. M. (2012). Structural equation modeling (pp. 671-675). In *Handbook of psychology* (2nd edition), Chapter 23.

Uluslararası Telekominikasyon Birimi, (2017). Gelişmiş, gelişmekte ve dünya genelindeki hanelerdeki internet erişim istatistikleri. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (Erişim tarihi: 12.05.2019).

Vacca, J. (2013). List of Security Products. In *Computer and information security handbook* (pp. e135-e137). Morgan Kaufmann.

Van Bavel, R., Rodríguez-Priego, N., Vila, J. and Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies,* 123, 29-39.

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J. and Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, 78, 283-297.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J. and Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75, 547-559.

Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security*, 77, 860-870.

Vroman, K. G., Arthanat, S. and Lysack, C. (2015). "Who over 65 is online?" Older adults' dispositions toward information communication technology. *Computers in Human Behavior*, 43, 156-166.

Walrave, M., Vanwesenbeeck, I. and Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 6 (1).

Weber, E. U., Blais, A. R. and Betz, N. E. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making*, 15 (4), 263-290.

Wheaton, B., Muthen, B., Alwin, D. F. and Summers, G. F. (1977). Assessing reliability and stability in panel models. *Sociological Methodology*, 8, 84-136.

White, C. M., Gummerum, M. and Hanoch, Y. (2015). Adolescents' and Young Adults' Online Risk Taking: The Role of Gist and Verbatim Representations. *Risk Analysis*, 35 (8), 1407-1422, DOI: 10.1111/risa.12369.

White, C. M., Gummerum, M., Wood, S. and Hanoch, Y. (2017). Internet safety and the silver surfer: The relationship between gist reasoning and adults' risky online behavior. *Journal of Behavior and Decision Making*, 30 (4), 819-827.

Worthington, R.L. and Whittaker, T.A. (2006). Scale development research: A content analysis and recommendations for best practices. *The Counseling Psychologist*, 34, 806-838.

Yenilmez, Y. and Seferoglu, S. S. (2013). An overview of teachers' awareness on cyberbullying. *Education and Science*, 38 (169), 420-432.

EKLER

EK-1**.** "Dijital Güvenlik Öz Yeterlik Ölçeği" Çalışma Yaprağı

Aşağıda dijital ortamlarda güvenlik becerilerinizi yansıtan ya da yansıtmayan ifadeler yer almaktadır. Lütfen her bir ifadenin yanına, o ifadenin sizi yansıtma düzeyini dikkate alarak, o ifadeye katılıp katılmadığınızı belirtmek için "Kesinlikle Katılmıyorum, Katılmıyorum, Kararsızım, Katılıyorum ve Kesinlikle Katılmıyorum" ifadelerinden uygun gördüğünüz seçimi yapıp, ilgili alanı "X" şekliyle işaretleyiniz.

Dijital güvenlik bilgi ve becerileri		**Açıklamalar**
İnternet Teknolojileri ve Veri Güvenirliği	1. Kullandığım telknolojiyi bilirim (dijital okuryazar olduğum teknolojiyi kullanırım)	
	2. İnternette herhangi bir oyun veya siteye üye olmadan önce ilgili profilimi nasıl sileceğimi bilirim	
	3. Bana gelen istenmeyen mesaj, e-postaları silebilirim.	
	4. Bana gelen zararlı içerikli e-postaları, reklam bağlantılarını, açılır pencereleri engelleyebilirim.	
	5. Bana uygun olmayan içeriklerde mesaj e posta fotograf gibi gönderenleri engelleyebilirim	
	6. İnternet erişimi olan teknolojik araçlarıma virüs programı kurabilirim.	
	7. Yangın, hırsızlık, hata, soyulma ya da kaybetme gibi durumlara karşı verilerimi farklı şekillerde yedekleyebilirimm.	
	8. İnternet erişimi olan teknolojik araçlarımda internet erişimini filtreleyen yazılımlar yükleyebilirim	
	9. Sanal Gizlillik Ağları (VPN-Virtual Private Networks) ayarlarımı yapabilirim.	
	10. İnternet erişiminde tarayıcımın güvenlik ayarlarını yapılandırabilirim.	
	11. Arama motorumun geçmiş ve gizlilik ayarlarını Seçenekler ya da Araçlar menülerini kullanarak yapılandırabilirim.	
	12. Kullandığım e-posta ya da anlık mesajlaşma hesapları sağlayıcılarımı Güvenli Soket Katmanına sahip servislerden (SSL, URLsinde "HTTPS" tarafından desteklenen, Gmail, RiseUp vb.) kullanabilirim.	
	13. Yenilenen virüslere karşı korunabilmek için düzenli olarak kullandığım yazılımları güncelleyebilirim.	
Şifreleme	14. Kişisel bilgisayarıma güvenli şifre oluşturabilirim.	
	15. İnternet erişim olan araçlarımı şifreleyebilirim.	
	16. İnternete erişimim olan her araçta farklı ve güçlü şifre oluşturabilirim.	
	17. Bilgisayar, telefon, harici bellek, dosyalar ve iletişim kurduğum hesapları şifreleyebilirim.	
	18. Sanal hesaplarımın birçoğunda aynı şifreyi kullanırım / Tüm şifrelerimi aynı olarak kullanmam.	
	19. Sanal ortamlarda oluşturduğum profillerde yüksek güvenirlik düzeyinde şifreler oluşturabilirim.	
	20. Ticari işlemlerde kartlarımda şifreleme ile ilgili güvenlik önlemlerini alabilirim. (3D güvenlik uygulamasını kullanabilirim.)	

Kişisel Bilgilerin Gizliliği ve Güvenliği	21. Sanal ortamlarda gerçek kimlik bilgilerimi (Ad Soyad, Kimlik Numarası) paylaşmamam gerektiğini bilirim.	
	22. Sanal ortamlarda adres, telefon numarası gibi gerçek iletişim bilgilerimi paylaşmam.	
	23. Sanal ortamlarda gerçek kimliğimi kötüye kullanabilcek (başka şirketlere bu bilgilerin satılması, aleyhinde kullanılması) üyeliklerde kimliğimi açığa çıkaracak bilgileri vermekten kaçınırım	
	24. Sanal ortamlarda bir şey yayınlamadan önce gizlilik ve güvenliğim için artı ve eksilerini düşünebilirm.	
	25. İnternet ortamlarında neleri ne kadar paylaşabileceğimi bilirim	
	26. Sosyal ağ profillerinde paylaşımlarımın kimler tarafından görülebileceğini belirlerim.	
	27. Üyesi olduğum sosyal ağların ya da oyunların güvenlik ayarlarını kendi tercihlerime göre ayarlayabilirim	
	28. İnternete erişimi olan teknolojik araçlarımdaki verilerin gizliliği ve güvenliğini korumak için önlemler alırım.	
	29. Profilimi ve profilimin içeriklerini özel olarak ayarlayabilirim.	
	30. Online ortamlarda profilimi görüntüleyebilecek arkadaşları eklemede seçici davranırım.	
Çevrimiçi Zorbalık ve Usulsüzlüğe karşı durma	31. İnternet ortamında karşılaştığım bir sıkıntı karşısında başvuracağım mecraları bilirim	
	32. İnternet ortamlarında karşılaşılan tehditler karşısında nasıl yanıt verileceğini bilirim	
	33. Başkalarının online davranışlarından şüphelendiğimde hukuki olarak başvuracağım yeri bilirim.	
	34. İnternette olumsuz olarak karşılaştığım durumlar karşısında ekran görüntüsü, e-posta çıktısı, ilgili durumu kanıt olarak kullanabilmek için kayıt altına alabilirim.	
	35. Karşılaştığım olumsuz bir durumda internet servis sağlayıcıma rapor gönderebilirim.	
Bilgilerin Doğruluğunun Teyidi	36. İnternette okuduğum bir haberin kim tarafından yayınlandığını bulabilirim.	
	37. İnternetten edindiğim bilginin hangi tarihte ve kim tarafından yayınlandığını araştırabilirim.	
	38. İnternette herhangi bir oyun veya siteye üye olmadan önce ilgili oyun veya site hakkında araştırma yapabilirim.	
	39. E-posta, anlık mesajlaşma ya da gezindiğim sitelerden gelen bağlantıları tıklamadan güvenilirliğinden emin olurum.	
	40. İnternet ortamından edindiğim bilgilerin doğruluğunu araştırırım.	
	41. Dijital ortamlardan edindiğim bilgilerin doğruluğunu çoklu kontrollerle deneytleyebilirim. (en az üç yerden bakmak)	
	42. Dijital teknolojilerde bir paylaşım yapmadan “teyit.org” gibi sitelerde haberin doğru olup olmadığınıkontrol edebilirim.	
Güvenli İnternet Gezinimi	43. İnternet ortamında yaptığım gezinimlerin dijital ayak izlerim olduğunu bilirim	
	44. Halka açık bilgisayarları kullanırken gizli modda arama yapabilirim. Gizli modda gezinirim.	
	45. İnternette kendime ait olmayan araçlardan erişim yaptığımda web geçmişimi silebilirim	

	46. İnternet kafelerde, yada başkasının erişimi olduğu bilgisayarlarda e-posta hesaplarımı açmam.	
	47. İnternet bağlantısının yavaşladığı durumlarda başka araçlardan internete erişmeye çalışırım.	
	48. Dijital ortamlardaki davranışlarımın (arama yapma, paylaşımda bulunma, yorum yapma alışveriş yapma vb.) nasıl yorumlandığını değerlendirebilirim.	
	49. "tor Browser Bundle" gibi anonim ağları kullanarak web de anonim gezinim yapabilirim	
	50. Bilgisayarınızın hafızasında tuttuğu tarama geçmişinizi ve çerezlerimi her web tarayıcıyı kullandığımda silebilirim.	
	51. CCleaner gibi uygulamalar kullanarak web geçmişimi, çerezlerimi ya da diğer arama izlerimi silebilirim.	

EK-2. Açımlayıcı Faktör Analizi İçin Kullanılan Veri Toplama Aracı

Sayın Öğrenci,

Anadolu Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalında tasarlanan bu bilimsel çalışmada üniversite öğrencilerinin internet ortamında hangi davranışlarda bulundukları ve bu davranışların sebeplerini irdelemek amaçlanmıştır.

Belirtilen amaç doğrultusunda alanyazın taraması yapılmış, geçerlilik ve güvenilirlik çalışmaları doğrultusunda anket soruları düzenlenmiştir. Anket dört bölümden oluşmaktadır. İlk bölümde demografik bilgileri belirlemeye yönelik sorular yer almaktadır. İkinci bölümde, üniversite öğrencilerinin dijital güvenlik öz yeterliklerine, üçüncü bölümde çevrimiçi etkinliklerine ilişkin maddeler yer almaktadır. Dördüncü bölümünde ise kişilik özelliklerine ilişkin maddeler yer almaktadır. Anketin doldurulması yaklaşık 15-20 dakika sürmektedir.

Bu araştırma tamamen bilimsel amaçlarla yapılmaktadır ve sizden toplanan verilerin gizliliği esas tutulmaktadır. Toplanan veriler hiçbir şekilde bilimsel araştırma dışı amaçlarla kullanılmayacak, üçüncü şahıs ve kurumlarla paylaşılmayacak ve raporların hiçbir yerinde katılımcıların kimliklerini açığa çıkaran bilgiler verilmeyecektir. Bu araştırmaya katılmak tamamen isteğinize bağlıdır. Bu anlamda bu araştırmaya katılım için onay verdiğiniz takdirde çalışmanın herhangi bir aşamasında herhangi bir sebep göstermeden onayınızı geri çekmek hakkına da sahipsiniz. Sizden anket maddelerinden görüşlerinize en uygun olan maddeleri işaretlemeniz ve anketin tüm bölümlerini eksiksiz doldurmanız istenmektedir. Çalışmaya katılmak istediğinizi belirtmek için aşağıdaki "Çalışmaya gönüllü olarak katılmak istiyorum" kutucuğunu onaylayınız.

Çalışmaya gönüllü olarak katılmak istiyorum ☐

Araştırmanın gerçekleştirilmesi içim gösterdiğiniz ilgi ve yardımdan dolayı şimdiden teşekkür eder, saygılarımı sunarım.

Araştırmacı: Arş. Gör. Canan ÇOLAK
Anadolu Üniversitesi, Eğitim Fakültesi
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Tel: 0-222-3350580/1979, Fax: 0-222-3350579, e-posta: canancolak@anadolu.edu.tr

BÖLÜM I. Kişisel Bilgi Formu

Aşağıda sizi tanımlayan ya da tanımlamayan birçok özellik bulunmaktadır. Lütfen her bir ifadenin yanına, o ifadenin sizi tanımlama özelliğini dikkate alarak işaretleyiniz ya da cevap veriniz.

Cinsiyetiniz	☐ Kadın ☐ Erkek	**Yaşınız**	..... (Lütfen belirtiniz)
Fakülteniz	..... (Lütfen belirtiniz)	**Bölümünüz**	..... (Lütfen belirtiniz)
Öğrenim Düzeyiniz	☐ Hazırlık ☐ 3. Sınıf ☐ 1. Sınıf ☐ 4. Sınıf ☐ 2. Sınıf ☐Diğer..... (Lütfen belirtiniz)	**İnterneti hangi sıklıkla kullanıyorsunuz?**	☐ Günde 5-7 saat ☐ Günde 3-5 saat ☐ Günde 0-2 saat ☐ Haftada 2-5 saat ☐ Haftada 0-2 saat ☐Diğer..... (Lütfen Belirtiniz)
İnternet erişimi sağladığınız araçlar nelerdir? (Birden fazla seçenek işaretleyebilirsiniz)	☐ Akıllı Telefon ☐ Tabet ☐ Bilgisayar ☐ Diğer..... (Lütfen belirtiniz)	**Kaç yıldır internet kullanıyorsunuz?**	☐ 0-1 yıl ☐ 2-3 yıl ☐ 4-5 yıl ☐ 6-7 yıl ☐ 8 yıl ve üzeri
İnterneti hangi amaçla kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)	☐ Çevrimiçi oyunlar oynamak ☐ Film, video izlemek ☐ Dosya (müzik, film vb.) indirmek ☐ Araştırma yapmak ☐ İletişim kurmak ☐ Haber okumak ☐Diğer..... (Lütfen belirtiniz)	**Nerede Yaşıyorsunuz?**	☐ Ailemle birlikte evde ☐ Üniversite kampüsünde yurtta ☐ Üniversite kampüsü dışında bağımsız evde ☐Diğer ..... (Lütfen belirtiniz)

BÖLÜM II. Dijital Güvenlik

Açıklama: Aşağıda dijital ortamlardaki dijital güvenlik becerilerinize ilişkin ifadeler yer almaktadır. Lütfen her bir ifadenin yanına, o ifadenin sizi yansıtma düzeyini dikkate alarak, o ifadeye katılıp katılmadığınızı belirtmek için **"Kesinlikle Katılmıyorum, Katılmıyorum, Kararsızım, Katılıyorum ve Kesinlikle Katılıyorum"** ifadelerinden uygun gördüğünüz seçimi yapınız. Seçiminizi ilgili alanı "X" şekliyle işaretleyerek belirtiniz.

Madde yanıtlarında **"1=Kesinlikle Katılmıyorum, 2=Katılmıyorum, 3=Kararsızım, 4=Katılıyorum ve 5=Kesinlikle Katılıyorum"** anlamı taşımaktadır.

	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1. Facebook, Instagram gibi ...	1	2	3	4	5
2. Web geçmişimi ...	1	2	3	4	5
3. Çevrimiçi hesaplarıma ...	1	2	3	4	5
4. Dijital araçlarımda ...	1	2	3	4	5
5. Cep No bilgimi kullanan ...	1	2	3	4	5
6. Web tarayıcıma ...	1	2	3	4	5
7. Dijital araçlarımın ...	1	2	3	4	5
8. Çevrimiçi uygulamaların ...	1	2	3	4	5
9. Sabit disk, taşınabilir bellek ...	1	2	3	4	5
10. Ağ bağlantımı gizleyerek ...	1	2	3	4	5
11. Çevrimiçi uygulamalarının ...	1	2	3	4	5
12. İstenmeyen reklam ...	1	2	3	4	5
13. Cep No bilgimi kullanan ...	1	2	3	4	5
14. iCloud, Google Drive gibi ...	1	2	3	4	5
15. Çevrimiçi uygulamaların, ...	1	2	3	4	5
16. İnternet çerezlerimi ...	1	2	3	4	5
17. Çevrimiçi alışveriş ve ...	1	2	3	4	5
18. Çevrimiçi uygulama ...	1	2	3	4	5
19. Dijital araçlarıma ...	1	2	3	4	5
20. İstenmeyen e-postaları ...	1	2	3	4	5
21. Dijital hesaplarıma erişim ...	1	2	3	4	5
22. İnternet erişiminde kullandığım ...	1	2	3	4	5
23. İnternette gezinirken güvenli ...	1	2	3	4	5
24. İstenmeyen arkadaşlık ...	1	2	3	4	5
25. Sabit disk, taşınabilir ...	1	2	3	4	5
26. Ağ bağlantımı şifreleyerek ...	1	2	3	4	5
27. Çevrimiçi hesaplarımdan ...	1	2	3	4	5
28. Çevrimiçi uygulamaların ...	1	2	3	4	5
29. İnternet gezinimlerimde ...	1	2	3	4	5
30. Dijital araçlarımdaki ...	1	2	3	4	5
31. Çevrimiçi uygulamalara ...	1	2	3	4	5
32. Web tarayıcımın özel bilgilerimi ...	1	2	3	4	5
33. İnternete bağlanırken ...	1	2	3	4	5
34. İnternet erişimi olan ...	1	2	3	4	5
35. İnternet tarayıcımın ...	1	2	3	4	5

BÖLÜM III. Çevrimiçi Etkinlikler

Açıklama: Aşağıda çevrimiçi ortamlarda gerçekleştirilen bazı etkinlikler yer almaktadır. Lütfen her bir maddede, o etkinliği lise yıllarınızda ve şimdi ne kadar sıklıkla gerçekleştirdiğinizi dikkate alarak iki ayrı değerlendirme yapıp, 1 ile 5 arasında bir puanı seçim yapınız. İfadelerde sizi en çok tanımlayan özelliği dikkate alarak, uygun gördüğünüz sıklık bölümünü "X" şeklinde işaretleyiniz.

Maddelerin yanıtlarında "1=Asla, 2=Nadiren, 3=Ara Sıra, 4=Çok Sık, 5= Her Zaman" anlamı taşımaktadır.

Lütfen Sıklık Belirtiniz	Şimdi						Lise Yıllarımda				
	Asla	Nadiren	Ara Sıra	Çok Sık	Her Zaman		Asla	Nadiren	Ara Sıra	Çok Sık	Her Zaman
1. İnternetteki gezinim ...	1	2	3	4	5		1	2	3	4	5
2. Çevrimiçi hesaplarımın ...	1	2	3	4	5		1	2	3	4	5
3. Alışveriş siteleriyle ...	1	2	3	4	5		1	2	3	4	5
4. Sosyal ağ hesaplarımın ...	1	2	3	4	5		1	2	3	4	5
5. Çevrimiçi ortamlarda ...	1	2	3	4	5		1	2	3	4	5
6. İnternetten tanıştığım ...	1	2	3	4	5		1	2	3	4	5
7. Dijital araçlarımı kullanırken ...	1	2	3	4	5		1	2	3	4	5
8. Özel bilgilerimi ...	1	2	3	4	5		1	2	3	4	5
9. Yazılımların korsan ...	1	2	3	4	5		1	2	3	4	5
10. İnternet erişimi olan ...	1	2	3	4	5		1	2	3	4	5
11. Başkalarına müstehcenlik, ...	1	2	3	4	5		1	2	3	4	5
12. Yüz yüze tanımadığım ...	1	2	3	4	5		1	2	3	4	5
13. Kişileri çevrimiçi ...	1	2	3	4	5		1	2	3	4	5
14. Dijital araçlarımı ...	1	2	3	4	5		1	2	3	4	5
15. Çevrimiçi uygulamaların ...	1	2	3	4	5		1	2	3	4	5
16. Çevrimiçi oyunlarda oyun ...	1	2	3	4	5		1	2	3	4	5
17. Güvenlik yazılımları ...	1	2	3	4	5		1	2	3	4	5
18. Başkalarının kimlik ...	1	2	3	4	5		1	2	3	4	5
19. Çevrimiçi ortamlar ...	1	2	3	4	5		1	2	3	4	5
20. Doğruluğundan emin ...	1	2	3	4	5		1	2	3	4	5
21. Çevrimiçi ortamlarda ...	1	2	3	4	5		1	2	3	4	5
22. Dijital araçlarımı ...	1	2	3	4	5		1	2	3	4	5
23. İnternet yüzünden ...	1	2	3	4	5		1	2	3	4	5
24. Siteleri kullanmak ...	1	2	3	4	5		1	2	3	4	5
25. Güvenlik sertifikası ...	1	2	3	4	5		1	2	3	4	5
26. Başkalarının şifrelerini ...	1	2	3	4	5		1	2	3	4	5
27. Çevrimiçi ortamlarda ...	1	2	3	4	5		1	2	3	4	5
28. Sahte hesaplarla ...	1	2	3	4	5		1	2	3	4	5
29. İnternetten ...	1	2	3	4	5		1	2	3	4	5
30. Çevrimiçi uygulamaların ...	1	2	3	4	5		1	2	3	4	5
31. Web siteleri ...	1	2	3	4	5		1	2	3	4	5
32. Web tarayıcımın ...	1	2	3	4	5		1	2	3	4	5
33. Başkalarının bilgilerini...	1	2	3	4	5		1	2	3	4	5
34. Çevremdekilerle iletişim ...	1	2	3	4	5		1	2	3	4	5
35. Çevrimiçi ortamlarda kan ...	1	2	3	4	5		1	2	3	4	5
36. Sosyal ağ hesaplarımı ...	1	2	3	4	5		1	2	3	4	5
37. Messenger, WhatsApp gibi ...	1	2	3	4	5		1	2	3	4	5
38. Dosya paylaşım siteleri ...	1	2	3	4	5		1	2	3	4	5
39. İnternette tanıştığım ...	1	2	3	4	5		1	2	3	4	5
40. İnternette karşılaştığım ...	1	2	3	4	5		1	2	3	4	5
41. Sitelere üye olurken ...	1	2	3	4	5		1	2	3	4	5
42. İnternet üzerinden ...	1	2	3	4	5		1	2	3	4	5
43. Ortak erişime açık ...	1	2	3	4	5		1	2	3	4	5
44. Sosyal ağlarda arkadaş ...	1	2	3	4	5		1	2	3	4	5

Lütfen Sıklık Belirtiniz	Şimdi						Lise Yıllarımda				
	Asla	Nadiren	Ara Sıra	Çok Sık	Her Zaman		Asla	Nadiren	Ara Sıra	Çok Sık	Her Zaman
45. Çeşitli sitelerden ...	1	2	3	4	5		1	2	3	4	5
46. Web tarayıcısı ...	1	2	3	4	5		1	2	3	4	5
47. Çevrimiçi hesaplarımda ...	1	2	3	4	5		1	2	3	4	5
48. İnternetteki bilgilerden ...	1	2	3	4	5		1	2	3	4	5
49. İnternette karşılaştığım ...	1	2	3	4	5		1	2	3	4	5
50. İnternetten indirdiğim ...	1	2	3	4	5		1	2	3	4	5

BÖLÜM IV. Kişilik Özellikleri

Aşağıda sizi tanımlayan ya da tanımlamayan birçok kişilik özelliği bulunmaktadır. "Kendimi *dışa dönük, istekli* olarak görürüm." şeklinde cümle içinde boş bırakılan alana maddelerdeki ifadeleri getirerek kişilik özelliklerinizi değerlendiriniz. Lütfen her bir ifadenin yanına, o ifadenin sizi tanımlama düzeyini dikkate alarak, 1 ile 7 arasında bir rakam yazınız.

Maddelerin yanıtlarında "**1 = Tamamen katılmıyorum, 2 = Kısmen katılmıyorum, 3 = Biraz katılmıyorum, 4 = Kararsızım, 5 = Biraz Katılıyorum, 6 = Kısmen katılıyorum, 7 = Tamamen katılıyorum**" anlamını taşımaktadır.

Kendimi ..... olarak görürüm:

1. _____ Dışa dönük, istekli
2. _____ Eleştirel, kavgacı
3. _____ Güvenilir, öz-disiplinli
4. _____ Kaygılı, kolaylıkla hayal kırıklığına uğrayan
5. _____ Yeni yaşantılara açık, karmaşık
6. _____ Çekingen, sessiz
7. _____ Sempatik, sıcak
8. _____ Altüst olmuş, dikkatsiz
9. _____ Sakin, duygusal olarak dengeli
10. _____ Geleneksel, yaratıcı olmayan

EK-3. Etik Kurul Belgesi

Kayıt Tarihi: 24.01.2017 Protokol No: 10680

ANADOLU ÜNİVERSİTESİ ETİK KURULU KARARI

ÇALIŞMANIN TÜRÜ:	BAP Projesi-Doktora Tez Çalışması
KONU:	Eğitim Bilimleri
BAŞLIK:	Üniversite Öğrencilerinin Çevrimiçi Risk Alma Eğilimlerinin Çeşitli Değişkenler Açısından İncelenmesi
PROJE/TEZ YÜRÜTÜCÜSÜ:	Doç. Dr. Işıl KABAKÇI YURDAKUL Yrd. Doç. Dr. Onur DÖNMEZ
TEZ YAZARI:	Canan ÇOLAK
ALT KOMİSYON GÖRÜŞÜ:	-
KARAR:	Olumlu

ETİK KURUL ÜYELERİ — **İMZA/ TARİH** 23.02.2017

Prof. Dr. Aydın AYBAR
Rektör Yardımcısı / Etik Kurul Başkanı

Prof. Dr. Hayrettin TÜRK
Fen Bil.(Fen Fak.)

Prof. Dr. Yusuf ÖZTÜRK
Sağlık Bil.(Ecz. Fak.)

Prof. Dr. Esra CEYHAN
Eğitim Bil. (Eğitim Bil. Ens.)

Prof. Dr. Bülent GÜNSOY
Sos. Bil.(İkt. Fak.)

Prof. Dr. Münevver ÇAKI
Güz. San. (Güz. San. Fak.)

EK-4. Anadolu Üniversitesi Araştırma Uygulama İzni

Ana. Üni. Evrak Tarih ve Sayısı: 06/04/2017-E.41228

T.C.
ANADOLU ÜNİVERSİTESİ REKTÖRLÜĞÜ
Genel Sekreterlik
Yazı İşleri Müdürlüğü

Sayı : 63784619-605.01
Konu : Canan ÇOLAK'ın Doktora Tezi
Uygulama İzin Talebi

EĞİTİM BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 06/04/2017 tarihli ve 40976 sayılı yazınız.

Enstitünüz Bilgisayar ve Öğretim Teknolojileri Eğitimi Doktora Programı öğrencisi Canan ÇOLAK'ın, danışmanlığını Doç. Dr. Işıl KABAKÇI YURDAKUL'un yaptığı "Üniversite Öğrencilerinin Çevrimiçi Risk Alma Eğilimlerinin Çeşitli Değişkenler Açısından İncelenmesi" başlıklı doktora tezi araştırmasının, 2016-2017 öğretim yılı Bahar dönemi ve 2017-2018 öğretim yılı Güz ve Bahar dönemlerinde Üniversitemiz 4 yıllık fakültelerinde öğrenim gören öğrencilerle gerçekleştirmesi Rektörlüğümüzce uygun görülmüştür.

Bilgilerinizi rica ederim.

e-imzalıdır
Prof. Dr. Aydın AYBAR
Rektör a.
Rektör Yardımcısı

Yunus Emre Kampüsü Tepebaşı/Eskişehir
Telefon No: +90 222 335 05 80/1352-1353 Faks No: +90 222 335 36 16
E-Posta: gensek@anadolu.edu.tr İnternet Adresi: www.anadolu.edu.tr

Bilgi İçin: Bediha AKSAN
Unvan: Büro Personeli
Telefon No: 1352

EK-5. Eskişehir Osmangazi Üniversitesi Araştırma Uygulama İzni

T.C.
ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ REKTÖRLÜĞÜ
(Genel Sekreterlik)

Sayı : 86930425-604/1268/2806 17/04/2017

Konu :Canan ÇOLAK'ın Doktora Tezi
Uygulama İzin Talebi

ANADOLU ÜNİVERSİTESİ REKTÖRLÜĞÜNE

İlgi :06.04.2017 tarih ve 63784619-605.01-E.33805 sayılı yazınız.

İlgi yazınıza istinaden Üniversiteniz Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Doktora Programı öğrencisi Canan ÇOLAK, danışmanlığını Doç. Dr. Işıl Kabakçı YURDAKUL'un yaptığı" Üniversite Öğrencilerinin Çevrimiçi Risk Alma Eğilimlerinin Çeşitli Değişkenler Açısından İncelenmesi" başlıklı tezinin 2016-2017 öğretim yılı Bahar dönemi ve 2017-2018 öğretim yılı Güz ve Bahar dönemlerinde Üniversitemiz 4 yıllık Fakültelerinde öğrenim gören öğrencilerle gerçekleştirilmesi talebi Rektörlüğümüzce uygun görülmüştür.

Bilgilerinize arz ederim.

Prof. Dr. Adnan KONUK
Rektör a.
Rektör Yardımcısı

Adres: Meşelik Yerleşkesi
26480 Eskişehir

Tel : 0 222 239 37 50 Dahili:5048
Fax: 0 222 239 10 74

EK-6. Doğrulayıcı Faktör Analizi ve Araştırma Verilerini Toplma İçin Kullanılan Veri Toplama Aracı

Sayın Öğrenci,

Anadolu Üniversitesi, Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalında tasarlanan bu bilimsel çalışmada üniversite öğrencilerinin internet ortamında hangi davranışlarda bulundukları ve bu davranışların sebeplerini irdelemek amaçlanmıştır.

Belirtilen amaç doğrultusunda alanyazın taraması yapılmış, geçerlilik ve güvenilirlik çalışmaları doğrultusunda anket soruları düzenlenmiştir. Anket dört bölümden oluşmaktadır. İlk bölümde demografik bilgileri belirlemeye yönelik sorular yer almaktadır. İkinci bölümde, üniversite öğrencilerinin kişilik özelliklerine, üçüncü bölümde dijital güvenlik öz yeterliklerine ilişkin maddeler yer almaktadır. Dördüncü bölümünde ise çevrimiçi etkinliklerine ilişkin maddeler yer almaktadır. Anketin doldurulması yaklaşık 15-20 dakika sürmektedir.

Bu araştırma tamamen bilimsel amaçlarla yapılmaktadır ve sizden toplanan verilerin gizliliği esas tutulmaktadır. Toplanan veriler hiçbir şekilde bilimsel araştırma dışı amaçlarla kullanılmayacak, üçüncü şahıs ve kurumlarla paylaşılmayacak ve raporların hiçbir yerinde katılımcıların kimliklerini açığa çıkaran bilgiler verilmeyecektir. Bu araştırmaya katılmak tamamen isteğinize bağlıdır. Bu anlamda bu araştırmaya katılım için onay verdiğiniz takdirde çalışmanın herhangi bir aşamasında herhangi bir sebep göstermeden onayınızı geri çekmek hakkına da sahipsiniz. Sizden anket maddelerinden görüşlerinize en uygun olan maddeleri işaretlemeniz ve anketin tüm bölümlerini eksiksiz doldurmanız istenmektedir. Çalışmaya katılmak istediğinizi belirtmek için aşağıdaki "Çalışmaya gönüllü olarak katılmak istiyorum" kutucuğunu onaylayınız.

Çalışmaya gönüllü olarak katılmak istiyorum ☐

Araştırmanın gerçekleştirilmesi için gösterdiğiniz ilgi ve yardımdan dolayı şimdiden teşekkür eder, saygılarımı sunarım.

Araştırmacı: Arş. Gör. Canan ÇOLAK
Anadolu Üniversitesi, Eğitim Fakültesi
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Tel: 0-222-3350580/1979, Fax: 0-222-3350579, e-posta: canancolak@anadolu.edu.tr

BÖLÜM I. Kişisel Bilgi Formu

Aşağıda sizi tanımlayan ya da tanımlamayan birçok özellik bulunmaktadır. Lütfen her bir ifadenin yanına, o ifadenin sizi tanımlama özelliğini dikkate alarak işaretleyiniz ya da cevap veriniz.

Cinsiyetiniz	☐ Kadın ☐ Erkek	**Yaşınız**	..... (Lütfen belirtiniz)
Fakülteniz	..... (Lütfen belirtiniz)	**Bölümünüz**	..... (Lütfen belirtiniz)
Öğrenim Düzeyiniz	☐ Hazırlık ☐ 1. Sınıf ☐ 2. Sınıf ☐ 3. Sınıf ☐ 4. Sınıf ☐Diğer..... (Lütfen belirtiniz)	**İnterneti hangi sıklıkla kullanıyorsunuz?**	☐ Günde 5-7 saat ☐ Günde 3-5 saat ☐ Günde 0-2 saat ☐ Haftada 2-5 saat ☐ Haftada 0-2 saat ☐Diğer..... (Lütfen Belirtiniz)
İnternet erişimi sağladığınız araçlar nelerdir? (Birden fazla seçenek işaretleyebilirsiniz)	☐ Akıllı Telefon ☐ Tabet ☐ Bilgisayar ☐ Diğer..... (Lütfen belirtiniz)	**Kaç yıldır internet kullanıyorsunuz?**	☐ 0-1 yıl ☐ 2-3 yıl ☐ 4-5 yıl ☐ 6-7 yıl ☐ 8 yıl ve üzeri
İnterneti hangi amaçla kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)		☐ Çevrimiçi oyun oynamak ☐ Film, video izlemek ☐ Dosya (müzik, film vb.) indirmek ☐ Araştırma yapmak ☐ İletişim kurmak ☐ Haber okumak ☐Diğer..... (Lütfen belirtiniz)	

BÖLÜM II. Kişilik Özellikleri

Aşağıda sizi tanımlayan ya da tanımlamayan birçok kişilik özelliği bulunmaktadır. "**Kendimi *dışa dönük, istekli* olarak görürüm.**" şeklinde cümle içinde boş bırakılan alana maddelerdeki ifadeleri getirerek kişilik özelliklerinizi değerlendiriniz. Lütfen her bir ifadenin yanına, o ifadenin sizi tanımlama düzeyini dikkate alarak, 1 ile 7 arasında bir rakam yazınız.

Maddelerin yanıtlarında "**1: Tamamen katılmıyorum, 2: Kısmen katılmıyorum, 3: Biraz katılmıyorum, 4: Kararsızım, 5: Biraz Katılıyorum, 6: Kısmen katılıyorum, 7: Tamamen katılıyorum**" anlamını taşımaktadır.

Kendimi ..... olarak görürüm:

1. _____ Dışa dönük, istekli
2. _____ Eleştirel, kavgacı
3. _____ Güvenilir, öz-disiplinli
4. _____ Kaygılı, kolaylıkla hayal kırıklığına uğrayan
5. _____ Yeni yaşantılara açık, karmaşık
6. _____ Çekingen, sessiz
7. _____ Sempatik, sıcak
8. _____ Altüst olmuş, dikkatsiz
9. _____ Sakin, duygusal olarak dengeli
10. _____ Geleneksel, yaratıcı olmayan

BÖLÜM III. Dijital Güvenlik

Açıklama: Aşağıda dijital ortamlardaki dijital güvenlik becerilerinize ilişkin ifadeler yer almaktadır. Lütfen her bir ifadenin yanına, o ifadenin sizi yansıtma düzeyini dikkate alarak, o ifadeye katılıp katılmadığınızı belirtmek için "**Kesinlikle Katılmıyorum, Katılmıyorum, Kararsızım, Katılıyorum ve Kesinlikle Katılıyorum**" ifadelerinden uygun gördüğünüz seçimi yapınız. Seçiminizi ilgili alanı "X" şekliyle işaretleyerek belirtiniz.

Madde yanıtlarında "1=Kesinlikle Katılmıyorum, 2=Katılmıyorum, 3=Kararsızım, 4=Katılıyorum ve 5=Kesinlikle Katılıyorum" anlamı taşımaktadır.	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1. Çevrimiçi alışveriş ...	1	2	3	4	5
2. Çevrimiçi hesaplarımdan ...	1	2	3	4	5
3. Cep No bilgimi kullanan ...	1	2	3	4	5
4. İstenmeyen arkadaşlık ...	1	2	3	4	5
5. Çevrimiçi hesaplarıma ...	1	2	3	4	5
6. Facebook, Instagram gibi ...	1	2	3	4	5
7. Çevrimiçi uygulamaların ...	1	2	3	4	5
8. Dijital hesaplarıma erişim için ...	1	2	3	4	5
9. Çevrimiçi uygulamaların, ...	1	2	3	4	5
10. Çevrimiçi uygulama ...	1	2	3	4	5
11. Cep No bilgimi kullanan ...	1	2	3	4	5
12. Dijital araçlarımın ...	1	2	3	4	5
13. İnternet erişimi olan ...	1	2	3	4	5
14. Sabit disk, taşınabilir ...	1	2	3	4	5
15. Dijital araçlarımdaki ...	1	2	3	4	5
16. Ağ bağlantımı ...	1	2	3	4	5
17. İnternet erişiminde kullandığım ...	1	2	3	4	5
18. İnternette gezinirken ...	1	2	3	4	5

Madde yanıtlarında "1=Kesinlikle Katılmıyorum, 2=Katılmıyorum, 3=Kararsızım, 4=Katılıyorum ve 5=Kesinlikle Katılıyorum" anlamı taşımaktadır.	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
19. Web tarayıcıma ...	1	2	3	4	5
20. Dijital araçlarımda ...	1	2	3	4	5
21. İnternet tarayıcımın ...	1	2	3	4	5
22. Ağ bağlantımı şifreleyerek ...	1	2	3	4	5
23. İstenmeyen reklam veya ...	1	2	3	4	5

BÖLÜM IV. Çevrimiçi Etkinlikler

Açıklama: Aşağıda çevrimiçi ortamlarda gerçekleştirilen bazı etkinlikler yer almaktadır. Lütfen her bir maddede, o etkinliği lise yıllarınızda ve şimdi ne kadar sıklıkla gerçekleştirdiğinizi dikkate alarak iki ayrı değerlendirme yapıp, 1 ile 5 arasında bir puanı seçim yapınız. İfadelerde sizi en çok tanımlayan özelliği dikkate alarak, uygun gördüğünüz sıklık bölümünü "X" şeklinde işaretleyiniz.

Maddelerin yanıtlarında "1: Asla, 2: Nadiren, 3: Ara Sıra, 4: Çok Sık, 5: Her Zaman" anlamı taşımaktadır.	Şimdi						Lise Yıllarımda				
	Asla	Nadiren	Ara Sıra	Çok Sık	Her Zaman		Asla	Nadiren	Ara Sıra	Çok Sık	Her Zaman
1. İnternetten tanıştığım ...	1	2	3	4	5		1	2	3	4	5
2. Sosyal ağlarda arkadaş ...	1	2	3	4	5		1	2	3	4	5
3. Çevrimiçi ortamlar aracılığıyla ...	1	2	3	4	5		1	2	3	4	5
4. İnternette tanıştığım kişilerle ...	1	2	3	4	5		1	2	3	4	5
5. Yüz yüze tanımadığım ...	1	2	3	4	5		1	2	3	4	5
6. Çevrimiçi ortamlarda tanımadığım ...	1	2	3	4	5		1	2	3	4	5
7. Çevrimiçi oyunlarda oyun ...	1	2	3	4	5		1	2	3	4	5
8. Web siteleri üzerinden ...	1	2	3	4	5		1	2	3	4	5
9. Alışveriş siteleriyle ikinci ...	1	2	3	4	5		1	2	3	4	5
10. Yazılımların korsan ...	1	2	3	4	5		1	2	3	4	5
11. Çevrimiçi uygulamaların ...	1	2	3	4	5		1	2	3	4	5
12. Messenger, WhatsApp gibi ...	1	2	3	4	5		1	2	3	4	5
13. Özel bilgilerimi ...	1	2	3	4	5		1	2	3	4	5
14. Çevrimiçi uygulamaların ...	1	2	3	4	5		1	2	3	4	5
15. Ortak erişime açık araçlarda ...	1	2	3	4	5		1	2	3	4	5
16. Başkalarının şifrelerini ...	1	2	3	4	5		1	2	3	4	5
17. Doğruluğundan emin ...	1	2	3	4	5		1	2	3	4	5
18. Başkalarına müstehcenlik, ...	1	2	3	4	5		1	2	3	4	5
19. Çevrimiçi ortamlarda ...	1	2	3	4	5		1	2	3	4	5

EK-7. “Çevrimiçi Risk Alma Eğilimi Ölçeği” Çalışma Yaprağı

Aşağıda çevrimiçi ortamlarda geçmişte ve son zamanlarda gerçekleştirdiğiniz ya da gerçekleştirmediğiniz birçok aktivite yer almaktadır. Lütfen her bir maddede, o aktiviteyi geçmişte ve son zamanlarda ne kadar sıklıkla katılım gösterme düzeyinizi dikkate alarak, o ifadeye katılıp katılmadığınızı belirtmek için 1 ile 5 arasında bir puanı seçiniz. İfadelerde size en çok tanımlayan özelliği dikkate alarak, uygun gördüğünüz rakam bölümünü “X” şeklinde işaretleyiniz.

Maddelerin yanıtlarında “1=Asla, 2=Nadiren, 3=Oldukça Sık, 4=Sık Sık, 5= Çok Sık” anlamı taşımaktadır.

Çevrimiçi Riskler Çerçevesi		**Açıklamalar**
Kişisel Bilgilerin Paylaşımı	1. Çevrimiçi ortamlarda veya e-posta yoluyla tanımadığım kişilerle çeşitli bilgilerimi (telefon numarası, adres, okul adı vb) paylaşırım	
	2. Dijital ortamlarda asla telefon numarm, adresim, okul adım, şifrem gibi kişisel bilgilerimi paylaşmam	
	3. İnternet üzerinden oyun oynarken kendim ve ailem hakkında fotoğraf, kişisel bilgi ve şifremi paylaşabilirim.	
	4. Çevrimiçi ortamlarda (web oyunları, sosyal ağlar vb.) telefon numaramı, ismimi gibi bilgilerimi ortamdan tanıştığım kişilere söylerim.	
	5. Ücretsiz oyun sağlayan bazı sitelere kişisel bilgilerimi kapsamlı bir şekilde vererek üye olurum	
	6. Ücretsiz oyunlara üye olmak için birçok detaylı bilgiyi içeren formları doldururum.	
	7. Sosyal ağlarda tanımadığım insanlarla kişisel bilgilerimi paylaşırım	
	8. Gerçek ismimi, yaşımı gibi bilgilerimi online ortamlarda herkesin görmesine izin veririm	
	9. Gerçek ismimi, yaşımı gibi bilgilerimi online ortamlarda tanımadığım kişilerin görmesine izin veririm	
	10. Online yazışma ortamlarında kendinizle ilgili bir şeyi temsil etmeyen bir takma ad kullanırım	
	11. Çevrimçi ortamlarda profillerimi herkesin görüntüleyebilmesine izin veririm	
	12. Birçok uygulama ve sosyal ağın konum bilgilerimi kullanmasına izin veririm	
	13. Birçok uygulama ve sosyal ağlarda nerede olduğumu gösteren paylaşımlarda bulunurum	
	14. Çevrimiçi ortamlarda kişisel fotoğraflarımı paylaşırım.	
Ticari İlgiler	15. Para kazanmak için bahis oyunlarının oynandığı sitelere üye olurum.	
	16. Çevrimiçi oyunlarda seviye atlamak için içeriğini bilmediğim reklamlara tıklarım.	
	17. İnternet üzerinden ailemin kredi kartı bilgilerini kullanarak onlardan habersiz alışveriş yaparım	
	18. Çevrimiçi ortamlarda kumar oynarım	
	19. Online oyunlarım ücretsiz olsa bile daha fazla hak kazanmak ya da yeni seviyeye geçebilmek için bazı öğeleri satın alırım	

	20. İnternette alışveriş (video oyunu alma vb., oyunlar için hak alma, silah alma) yaparken ailemin kredi kartını kullanırım	
Güvenlik	21. Güvenliğinden emin olmadığım dosya paylaşım sitelerini kullanırım	
	22. E-postama gelen bilmediğim kişilerin paylaştığı linkleri görüntülerim	
	23. Çevrimiçi ortamlardan müzik, video ve diğer dosyaları indiririm	
	24. İnternete erişim sağladığım araçlara virüs programı kurarım	
	25. İnternete erişimimi sağlarken uygun olmayan içerikleri engellemek için filtreli internet kullanırım	
	26. Çevrimiçi ortamlarda profil oluşturduğum her ortamın güvenlik ayarlarını kontrol etmem	
	27. Çevrimiçi ortamlarda profil oluşturduğum her ortamın gizlilik ayarlarını kontrol etmem	
	28. Çevrimiçi ortamlardan çeşitli uygulamaları indiririm	
Zorba Olma	29. Çevrimiçi ortamlarda başkalarının hesap şifrelerini alabilirim	
	30. İnternet üzerinde başkalarına lakaplar takarım	
	31. İnternet üzerinde başkalarını küçük düşürücü şakalar yaparım ve paylaşırım	
	32. Çevrimiçi sohbet ortamlarında bir arkadaşımın kimliğini kullanırım.	
	33. Sosyal ağlarda (Facebook, Twitter vb.) arkadaşlarımı kızdıracak yorumlar yaparım.	
	34. Çevrimiçi ortamlarda karşımdakine kızdığımda uygun olmayan kelimeler sarfederim.	
	35. Çevrimiçi ortamlardaki arkadaşlarım fotoğrafları üzerinde oynayarak başka sitelerde yayınlarım.	
	36. Çevrimiçi ortamlarda başka kimlikle arkadaşlarımı tehdit ederim	
	37. Arkadaşlarıma içeriğinde cinsel öğeler olan (Fotoğraf, video vb.) e-posta gönderirim.	
	38. Dijital ortamlarında başkalarına saygılı ve kibar olurum	
	39. Yüzyüze söyleyemeyeceğim bir şeyi dijital ortamlar aracılığıyla başkalarıyla paylaşmam	
	40. İnternette başkalarını rahatsız edebilecek iğneleyici bir dil kullanırım	
	41. İnternette tanımadığım kişilerin neler yaptıklarını izni olmadan takip ederim	
	42. Whatsup gruplarında tanımadığım numaraları ararım.	
Çevrimiçi Yabancılarla İletişim ve Etkileşim	43. İnternet üzerinden tehdit edildiğimde tehdit edenin isteklerini yaparım	
	44. Çevrimiçi ortamlarda tanıştığım kişilerle görüntülü iletişim kurarım.	
	45. Çevrimiçi ortamlarda tanıştığım kişilerle yazılı iletişim kurarım.	
	46. Çevrimiçi tanıştığım kişilerle arkadaş olup dışarıda sosyalleşirim.	
	47. Çevrimiçi ortamlarda tanıştığım kişilere uygun olmayan fotoğraflar gönderirim.	
	48. Çevrimiçi ortamlarda tanıştığım kişilerin verdikleri bilgilere güvenirim (cinsiyet yaş vb.)	
	49. İnternette tanımadığım kişilerle sohbet ederim	
	50. Çevrimdışı ortamlarda kemdimden yaşça büyük kişilerle haberleşirim	
	51. Çevrimiçi ortamlarda tanımadığım kişilerden gelen arkadaşlık tekliflerini kabul ederim	
	52. Sosyal ağlarda tanımadığım insanlardan gelen arkadaşlık tekliflerini kabul ederim	
	53. Online oyunlarda tanımadığım insanlardan gelen arkadaşlık tekliflerini kabul ederim	

	54. Online oyunlarda tanımadığım insanlaral yüz yüze tanışırım	
	55. Online ortamlarda edindiğim arkadaşlarla tek başıma buluşmam.	
Doğru Olmayan Bilgi Paylaşımı ve Edinimi	56. Çevrimiçi ortamlarda kendimi farklı cinsiyetle tanıtırım	
	57. Yaş sınırı olan sitelere üye olurum	
	58. İnternetten edindiğim bilgilerin doğruluğunu kontrol etmem	
	59. Üyesi olduğum sanal ortamlarda (sosyal ağlar, sanal dünyalar, internet oyunları) yanlış bilgi içeren haberler yayınlarım.	
	60. İnternetteki yaş sınırlamaları olan web sitelerine üye olurum	
	61. İnternetteki yaş sınırı olan oyunlara üye olurum	
	62. Yaşıma uygun olmayan oyunlara üye olurum	
	63. Çevrimiçi ortamlarda trol haberler yayınlarım	
	64. Çevrimiçi ortamlarda doğruluğundan emin olmadığım bilgileri yayınlarım	
	65. Ödevlerimi yaparken internetten edindiğim bilgileri kontrol etmeden kullanırım	
Uygun Olmayan İçerik Arama, Görüntüleme ve Gönderme	66. Yaşıma uygun olmayan çevrimiçi içerikleri görüntülerim	
	67. Uygunsuz içerikli mesajlar alırım	
	68. Uygunsuz içerikli mesajlar gönderirim	
	69. Arama motorlarında cinsel içerik (Fotoğraf, video vb.) ararım.	
	70. Çevrimiçi ortamlarda kumar oyunlarını araştırırım	
	71. Çevrimiçi oyunlarda şiddet içerikli olan oyunları oynamayı tercih ederim	
	72. Çevrimiçi ortamlarda şiddet içerikli olan görsel videoları görüntülerim	
	73. İnternette yasal olmayan çocuk istismarı hakkında görsellerle karşılaşırım	
	74. İnternette zayıflamak/şişmanlamak için önerilen ilaçlarla ilgili bilgileri takip ederim	
	75. İnternette kendinde zarar verme konusundaki metin, görsel ve resimleri görüntülerim	
	76. İnternette intihar etme ile ilgili içerikleri görüntülerim	
Online Aktivitelerin	77. Çevrimiçi ortamlarda rahatsız olduğum konular hakkında kimseyle iletişim kurmam	
	78. İnternet ortamlarında karşılaştığım olumsuz durumları ailemle, öğretmenimle paylaşırım	
	79. Çevrimiçi ortamlarda karşılaştığım olumsuz durumları akranlarımla paylaşırım	
	80. İnternette gördükleriniz ya da karşılaştıklarınızı ile ilgili kendinizi rahatsız hissettiğinizde aileme ya da ebeveynlerimle bunu konuşabilirim	
Sağlık	81. İnternet teknolojilerini kullanırken fiziki duruşumu kontrol ederim.	
	82. Gün içerisinde vaktimin çoğunu internette, internet uygulamalarıyla geçiririm.	
	83. Gün içerisinde üyesi olduğum dijital ortamları (oyun, sosyal medya vb.) sürekli takip ederim.	
	84. Dijital ortamları kullanırken zamanın nasıl geçtiğini farketmem.	

ÖZGEÇMİŞ

Adı Soyadı : Canan ÇOLAK

Yabancı Dil : İngilizce

Doğum Yeri ve Yılı : Trabzon / 1987

E-posta : canancolak@anadolu.edu.tr

Eğitim ve Mesleki Gelişimi:

- 2013, Karadeniz Teknik Üniversitesi, Fatih Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı (Yüksek Lisans)
- 2010, Dokuz Eylül Üniversitesi, Eğitim Fakültesi, Bilgisyaar ve Öğretim Teknolojileri Eğitimi Bölümü (Lisans)
- 2018, Araştırma Görevlisi, Giresun Üniversitesi, Eğitim Fakültesi
- 2014, Araştırma Görevlisi, Anadolu Üniversitesi, Eğitim Fakültesi
- 2012, Araştırma Görevlisi, Karadeniz Teknik Üniversitesi, Eğitim Fakültesi
- 2011, Araştırma Görevlisi, Giresun Üniversitesi, Eğitim Fakültesi

Yayınları ve Bilimsel Faaliyetleri:

- Ebeveynlerin Dijital Vatandaş Yetiştirme Yeterliklerini Geliştirmeye Yönelik Bir Eğitim Ortamının Geliştirilmesi, TÜBİTAK PROJESİ
- Kurt, A. A., Çolak, C., Dönmez, P., Filiz, O., Türkan, F., ve Odabaşı H. F. (2016). Opportunities for students with disabilities in higher education institutions in Turkey: Where is ICT. *International Journal of Special Education, 31*(1), 104-113.
- Karal, H., Kokoç, M., Çolak, C., ve Yalçin, Y. (2015). A Case study on online mathematics teaching with pen-based technology experiences of two instructors. *Contemporary Educational Technology, 6*(4), 319-337.
- Karal, H., Kokoç, M., Çolak, C., ve Yalçin, Y. (2013). Using pen-based technology in online mathematics course: An evaluation study. *European Journal of Open, Distance and E-learning, 16(*2), 152-164.
- Baran, B., Çukurbaşi, B., Çolak, C., ve Doğusoy, B. (2012). Second Life users' profiles and views about educational potential of Second Life: A case of Turkey. *The Turkish Online Journal of Educational Technology, 11*(4), 253-263.
- Yaman, F., Avci, E., Dönmez, O., Çaktu Dönmez, P., Çolak, C., ve Kabakçi Yurdakul, I. (2018). Dijital Ebeveynlik Eğitim Ortamının Tasarlanması Süreci. 12. Uluslararası Bilgisayar ve Öğretim Teknolojileri Eğitimi Sempozyumu.
- Çolak, C., Dulkadir N., ve Kabakçi Yurdakul, I. (2017). Öğretmen Adaylarının Dijital Yerlilik Algıları. 5. Uluslararası Öğretim Teknolojileri ve Öğretmen Eğitimi Sempozyumu.

- Controversial Issues in Social Studies Education in Turkey: The Contemporary Debates, Bölüm adı: (Digital Divide in Social Studies Education) (2018)., Çolak C., Karaduman H., Kabakçı Yurdakul, I., Information Age Publishing, Editör: Elvan Günel, Basım sayısı:1, Sayfa Sayısı 270, ISBN:1641133058, İngilizce.