Eğitim Fakültesi Öğrencileri ile Diğer Fakültelerdeki Öğrencilerin Siber Güvenlik Farkındalıklarının Karşılaştırılması

Ali Semerci [1]

Özet: Son yıllarda siber ortamların hayatı ilgilendiren her alanda gerçek hayata kıyasla daha fazla kolaylık, konfor ve kazanç sağlamakla birlikte bazı riskleri de beraberinde getirdiği görülmektedir. Farklı gerekçelerle zamanlarının önemli bölümünü bu ortamlarda geçiren kullanıcıların siber güvenlik farkındalıklarının düşük olması çoğu zaman ciddi mağduriyetler yaşanmasına neden olmaktadır. Siber güvenlik siber uzayı kullanan tüm bireyler için önemli olmakla birlikte öğretmenlere daha fazla görev ve sorumluluk düşmektedir. Bu araştırmada öğretmen adayı eğitim fakültesi öğrencilerinin siber güvenlik farkındalık düzeylerinin diğer fakülte öğrencilerinin farkındalık düzeyleriyle karşılaştırılması ve farklı değişkenler açısından incelenmesi amaçlanmıştır. Araştırma, tarama modelinde gerçekleştirilmiştir. Çalışma grubunu 2018-2019 eğitim-öğretim yılında üç farklı devlet üniversitesinde öğrenim gören 448 üniversite öğrencisi oluşturmuştur. Veriler, anket formu ve *"Kişisel Siber Güvenliği Sağlama Ölçeği"* kullanılarak toplanmıştır. Araştırma bulguları, katılımcıların kişisel siber güvenlik farkındalıklarının orta ve üzeri düzeyde olduğu, eğitim fakültesi öğrencilerinin siber güvenlik farkındalık düzeyleri ile diğer fakültelerdeki öğrencilerin farkındalık düzeyleri ve cinsiyet arasında anlamlı farklılık bulunmadığı sonucuna ulaşılmıştır. Öğrencilerin siber güvenlik farkındalıkları ile sınıf düzeyi ve günlük internet kullanım süreleri arasında farklı etki düzeylerinde anlamlı farklılık bulunmuştur.

Anahtar Kelimeler: Siber güvenlik, siber güvenlik farkındalığı, üniversite öğrencileri, öğretmen adayları.

DOI: 10.29329/mjer.2019.210.8

Comparison of Cybersecurity Awareness of Education Faculty Students with Students of Other Faculties

Abstract: In the information age, cyber environments provide great convenience, comfort and gain in all areas of life compared to real life. However, cyber space may subject to some risks and dangers. The low level cybersecurity awareness of users spending significant amount of time in cyberspace for many different reasons can lead to serious grievances. The fact that children and young people are more likely to be at risk in cyber space imposes important duties and responsibilities to the teachers at all levels to raise cybersecurity awareness of their students. In this regard, the present study aimed to compare the personal cyber security awareness levels of students attending teacher training program in education faculties and students from other faculties. The research was carried out in survey model. The study group consisted of 448 university students from three different public universities in the 2018-2019 academic year. Data were collected through a questionnaire and "Personal Cyber Security Scale". The findings of the study showed that the participants' cyber security awareness was moderate and above, and there were no significant differences between gender and the

1 **Ali Semerci,** Dr., Elmadağ Şehit Mustafa Büyükpoyraz P O M E M, Elmadağ Şehit Mustafa Büyükpoyraz P O M E M, ORCID: 0000-0002-8495-0147

İrtibat Yazarı: alisemerci@hotmail.com

cybersecurity awareness levels of the prospective teachers who were continuing their education in different programs of education faculties and the awareness levels of students in other faculties. Significant differences were found between students' cyber security awareness levels and grade level and daily internet usage time variables.

Keywords: Cybersecurity, cybersecurity awareness, university students, pre-service teachers

GİRİŞ

İçinde bulunduğumuz bilgi ve teknoloji çağının bir gereği olarak bireyler, şirketler, kurum ve kuruluşlar her türlü iş ve işlemi elektronik ortamlarda gerçekleştirmektedir. Bu ortamlar bireylere gerçek hayatta gerçekleştirdikleri birçok faaliyeti daha rahat ve konforlu bir şekilde yapma, işletmelere daha fazla hareket alanı, müşteri ve kazanç, kurumlara ise daha etkin, kaliteli ve verimli hizmet sunma fırsatları sağlamaktadır. Siber ortamların sunduğu sayısız fırsatlarla önemli bir cazibe alanı haline gelirken, bu ortamlardaki ekonomik hareketliliğin boyutu, suç işlemenin gerçek hayata kıyasla daha kolay olması, suçluların tespit edilmesindeki zorluklar, ulusal ve uluslararası yasal boşluklar gibi nedenlerle siber suçlular için de cazip hale gelmiştir. Bu durum, siber uzayda işlenen suçların her geçen gün yenileri eklenerek artmasına neden olmaktadır (Gönen, Ulus ve Yılmaz, 2016; Moore, 2014).

İnsanlığın ortak hafızası olarak nitelendirilen siber uzayda (Erdem ve Özocak, 2019) bireysel ya da kurumsal kullanıcıların önceden gerekli siber güvenlik önlemleri almak yerine ciddi bir sorunla karşı karşıya kaldıktan sonra harekete geçme eğiliminde oldukları görülmektedir (Yılmaz, Şahin ve Akbulut, 2016). Bu durum kullanıcıların çoğu zaman öngörülemez derecede yıkıcı sonuçları olan tehlikelerle karşı karşıya kalmalarıyla sonuçlanmaktadır (Rand Europe Report, 2014). Bu tehlikeler zamanlarının büyük bölümünü alışveriş, oyun, eğlence, sosyalleşme gibi farklı gerekçelerle siber ortamlarda geçiren çocuk ve gençler (Parlak-Yorğancı, 2018) açısından daha olumsuz sonuçlar doğurabilmektedir (Farrukh, Sadwick ve Villasenor, 2014). Ülkemizin en çok siber saldırıya maruz kalan ve düzenlenen siber saldırılardan en çok etkilenen ülkelerin başında gelmesi (STM, 2018; TrendMicro, 2019) içinde bulunduğumuz tehlikenin boyutunu ortaya koymaktadır.

Siber uzay başta ekonomik nedenler olmak üzere, meydan okuma, merak ve eğlence, intikam, kendini kabul ettirme, casusluk, terörizm, ve radikalizm gibi farklı motivasyonlarla siber saldırganlar için yeni fırsatları yaratırken, bireysel ve kurumsal kullanıcılar bakımından her geçen gün daha riskli hale gelmektedir (Li, 2017; Sabillon vd., 2016; STM, 2018). Saldırganlar zararlı programlar, tuş ve ekran kaydediciler, sosyal mühendislik ve oltalama gibi farklı yöntem ve tekniklerle siber uzayda amaçlarına ulaşmaya çalışmaktadır (Brar ve Kumar, 2018; Sağıroğlu, 2018). Siber uzayda sıklıkla karşılaşılan çocukların istismarı, zorbalık, uyuşturucu ticareti, sanal kumar, nitelikli dolandırıcılık ve kimlik hırsızlığı gibi suçlara (UNICEF, 2017) her geçen gün yenileri eklenmeye devam etmektedir.

Siber ortamlarda özellikle çocuk ve gençlerin kendilerine zarar verme, intihara teşvik, riskli cinsel etkileşimlere yönlendirilme, saldırganlara güvenerek gelecekte özel hayat ve kariyerlerini tehlikeye atabilecek nitelikte paylaşımlar yapmaya zorlanma gibi durumlara sürüklendikleri görülmektedir (Kavuk, Keser ve Teker, 2011; Bulu, Kavuk-Kalender ve Keser, 2017). Bu ortamlarda mağduriyet yaşayan bireylerin suç teşkil eden durumlara karşılık verme ya da intikam duygusu çoğu zaman onları aynı zamanda suçlu durumuna düşürmektedir (Semerci, 2016). Bu durum siber uzaydaki tehlikenin boyutunu artırmakta ve daha karmaşık hale gelmesine neden olmaktadır.

Bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme, banka veya kredi kartlarının kötüye kullanılması, yasak cihaz veya programlar kullanılması gibi suçlar Türk Ceza Kanunu'nda bilişim suçu olarak düzenlenmiştir. Bununla birlikte, çocukların cinsel istismarı, hakaret, tehdit, şantaj, nitelikli hırsızlık, nitelikli dolandırıcılık, telif hakları ihlali, ırkçılık ve nefret söylemleri gibi gerçek hayatta suç teşkil eden suçların tamamı bilişim sistemleri aracılığıyla işlenmesi durumunda suç olarak kabul edilmiş ve cezai yaptırım getirilmiştir (Türk Ceza Kanunu, 2014). Yasal düzenlemelerle getirilen yaptırımlara, farklı düzeylerdeki eğitim kurumlarının farkındalık kazandırmaya yönelik faaliyetlerine, ilgili kurum ve kuruluşlarca yapılan tüm uyarılara rağmen çocuk, genç, yaşlı, eğitimli, eğitimsiz, kadın ya da erkek ayrımı olmaksızın her geçen gün siber suç mağdurlarının sayısı artarak devam etmektedir.

Bu mağduriyetlerin temelinde kullanıcıların siber uzaydaki risk ve tehlikelere ilişkin farkındalık düzeylerinin yetersiz kaldığı gerçeği yatmaktadır (Çubukçu ve Bayram, 2013; Karaoğlan Yılmaz, Yılmaz ve Sezer, 2014; Yılmaz vd., 2016). Siber ortamların güvenli kullanımına ilişkin gerekli bilgi, beceri ve deneyime sahip olmayan, bir başka ifade ile siber güvenlik farkındalık düzeyi düşük kullanıcılar tehdit ve tehlikelere karşı daha savunmasız kalabilmektedir (Yiğit ve Seferoğlu, 2019). Kullanıcıların siber güvenlik farkındalıklarının düşük olması ise çoğu zaman ileri düzey teknik bilgiye bile sahip olmayan siber saldırganların işini kolaylaştırmaktadır.

Milyonlarca lira servet vadeden e-posta eklerinin açılması, ilgi çekici bir resmin tıklanması, merak edilen bir bağlantının yönlendirmesi ya da telefonda kendini otorite figürü olarak tanıtan dolandırıcıların psikolojik baskı ve ikna yöntemleri bireylerin tuzağa düşürülmesi için yeterli olabilmektedir. Farklı şekillerde amacına ulaşan saldırganlar bireylerin, işletmelerin, kurum ve kuruluşların ciddi maddi kayıplar yanında imaj ve itibar kaybı yaşamalarına neden olabilmektedir. Bilişim teknolojisi araçlarının hayatımızın ayrılmaz bir parçası haline gelmesi, bireylerin zamanının büyük bölümünü siber ortamlarda geçirmeye başlaması siber güvenliğin önemini her zamankinden daha fazla ön plana çıkarmıştır.

Siber güvenlik, Sağıroğlu (2018) tarafından "siber ortamlarda karşılaşılabilecek tehdit ve tehlikeler ile oluşabilecek riskleri önceden öngörüp bunlara karşı önceden önlem alma girişimi" veya "siber ortamlarda oluşacak riskleri minimize etmek ve yönetmek" şeklinde tanımlanmıştır. Siber

güvenliğin sağlanmasında kuşkusuz teknolojik tedbirler önemli yer tutmaktadır. Bununla birlikte, Keser ve Güldüren (2015) siber güvenliğin sağlanmasında önceliğin insan unsurunda olduğuna vurgu yaparak siber güvenlik farkındalığının kazandırılmasının önemine işaret etmektedir.

Güvenlik davranışının bir alt aşaması olarak değerlendirildiğinde farkındalık, siber güvenlik davranış düzeylerinin belirlenmesine temel teşkil etmektedir. Davranışın oluşmasında bireylerin olası tehditleri belirleyebilmesi, saldırı evreninde yer alan tehditlerden kendi varlıklarına yönelik olanları algılayabilmesi, sahip olduğu farkındalık derecesine göre tehdidin ortaya çıkarabileceği riskleri ve sonuçlarıyla risk unsurlarının giderilmesine yönelik gerçekleştirmesi gereken davranışa karar vermesini içeren dört aşamalı bir süreç bulunduğu görülmektedir (Erol ve Sağıroğlu, 2018). Benzer şekilde, Çatak ve Ögel (2010) duyarlılığı yüksek olan bireylerin dikkat ve farkındalıklarının yüksek olacağı gerçeğinden hareketle, siber ortamlarda kullanıcıların kendileri için tehdit ve tehlike oluşturabilecek durumları algılamaları, farkında olmaya yönelik dikkati yüksek tutmalarının önemine işaret etmektedir. Başka bir ifadeyle siber ortamlarda riskleri en aza indirmenin yolu sistemin en zayıf halkası durumundaki kullanıcıların siber güvenlik farkındalıklarının arttırılmasından geçmektedir (Yılmaz vd., 2016).

İçinde bulunduğumuz çağda, teknoloji kullanımı hayatın tüm alanları ve tüm meslekler için önemli hale gelmiştir. Bununla birlikte, bilişim teknolojilerinin eğitimin her alanını doğrudan etkilemesi eğitimde siber güvenlik, bilişim ve bilgi güvenliği gibi güvenlikle ilgili konuları öğretmenler açısından daha önemli hale getirmiştir. Öğretmenler görev yaptıkları süre içerisinde atama, yer değiştirme, görevlendirme, izin işlemleri, sınav başvuruları, hizmetiçi eğitim faaliyetleri gibi özlük ve kişisel bilgilerine ilişkin çok sayıda iş ve işlemlerini elektronik ortamda Milli Eğitim Bakanlığı Bilişim Sistemleri (MEBBİS) üzerinden yapmak zorundadır. Öğretmenlerden ayrıca, MEBBİS sistemi içerisinde yer alan e-Okul, hizmetiçi eğitim modülü, e-Akademi modülü, RAM modülü, EgiTek sınav modülü gibi 70'in üzerindeki modülü gerektiği durumlarda kullanmaları beklenmektedir (MEBBİS, 2015).

Milli Eğitim Bakanlığınca her öğrenciye eğitimde fırsat eşitliği sağlanarak nitelikli eğitim hizmeti sunulması amacıyla dünyanın en kapsamlı eğitime teknoloji entegrasyonu projesi olarak değerlendirilen Fırsatları Arttırma ve Teknolojiyi İyileştirme Hareketi (FATİH) projesi 2010 yılı itibariyle başlatılmıştır. Projeyle ülke genelindeki okulların her sınıfı için bilişim teknolojisi donanımı, yazılımı, ağ altyapısı ve internet erişim imkânı sağlanmış, öğrenci ve öğretmenlere tablet bilgisayarlar dağıtılarak eğitim bilişim ağı (EBA) üzerinden e-içeriklere erişim imkânı sağlanmıştır (MEB, 2019). Öğretmenlerden sağlanan bilişim teknolojisi imkânlarını eğitim süreçlerinde etkin, verimli ve güvenli şekilde kullanmaları ve aynı zamanda öğrencilerine örnek olmaları beklenmektedir. Diğer taraftan bilişim teknolojisi alanındaki çağdaş gelişmelerin eğitim süreçlerine yansıtılması yeni kuşakların farklılaşan eğitim alışkanlıkları ve beklentileri açısından büyük önem taşımaktadır. Yeni kuşak

öğrencilerin düşünme, bilgiye erişim, bilgiyi işleme ve öğrenme tercihleri ile öğretmen ve öğretim ortamlarından beklentileri farklılaşmıştır (Bilgiç, Duman ve Seferoğlu, 2011). Elektronik öğrenme platformları ve öğrenen merkezli yaklaşımlar öğrencilerin öğrenme tercihleri arasında ön plana çıkmıştır.

Hayatın her alanında olduğu gibi eğitimin her aşamasında teknolojinin yoğun kullanımı öğretmenlerin ve aynı zamanda öğretmen adaylarının siber güvenlik farkındalıklarının arttırılmasına yönelik eğitimin gerekliliğini ortaya çıkarmıştır. Yılmaz ve diğerleri (2016) tarafından da vurgulandığı şekilde öğretmenlerin siber ortamlardaki dijital veri güvenliği ve siber güvenlikle ilgili konulardaki karşılaşabilecekleri tehdit ve tehlikeleri bilmeleri, doğabilecek sorunların önlenebilmesi ya da en azından asgari düzeye indirilmesi açısından büyük önem taşımaktadır. Siber ortamların içerdiği riskler günümüz öğrencilerini içinde bulunduğumuz çağda siber ortamlarda sunulan olanaklardan mahrum etme gerekçesi olamayacağına göre, onların siber ortamların risklerinden azami ölçüde korunmalarını ve aynı ölçüde yararlanmalarını sağlayacak arayışlara yöneltmektedir.

Güvenli internet kullanımına ilişkin yasal düzenlemelere, alınan tedbirlere ve eğitim faaliyetlerine (Bıçakcı, Ergun ve Çelikpala, 2015; GüvenliWEB, 2019) rağmen yapılan araştırmalar, istatistiki veriler ve yaşanan olaylar bu çabaların yetersiz kaldığını ortaya koymaktadır. Bu durum, kullanıcıların siber güvenlik farkındalık düzeylerinin arttırılmasına yönelik çalışmaların arttırılması gerekliliğini beraberinde getirmektedir. Alan yazında, üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin belirlenmesine, farkındalık düzeyleriyle kişilik özellikleri, yaş, cinsiyet, sınıf düzeyi, bölüm, bilişim güvenliği eğitimi alma durumu ve internet kullanım süresi gibi değişkenler açısından incelenmesine ilişkin araştırmalar bulunmaktadır. Bu araştırmaların bazılarında üniversite öğrencilerinin siber güvenlik davranış düzeylerinin yeterli olduğu sonucuna ulaşıldığı görülmektedir (Karacı, Akyüz ve Bilgici, 2017; Yiğit ve Seferoğlu, 2019). Çok sayıdaki araştırma bulgusu ise üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin yetersiz olduğunu ortaya koymuştur (Akgün ve Topal, 2015; Bulu vd., 2017; Gökmen ve Akgün, 2016; Karaoğlan Yılmaz vd., 2014; Pusey ve Sadera, 2011; Tekerek ve Tekerek, 2013). Alan yazında konuya ilişkin olarak gerçekleştirilen bu araştırmaların büyük çoğunluğunda bilgi güvenliği ve siber güvenlik farkındalığının arttırılmasına yönelik eğitimlerin gerekliliğine vurgu yapıldığı görülmektedir.

Siber güvenlik farkındalığına ilişkin araştırmalarda ulaşılan farklı sonuçlar yanında, bilişim teknolojisi alanındaki hızlı gelişmelerin ihtiyaç ve riskleri her geçen gün farklılaştırması siber güvenlik farkındalık ve davranış düzeylerinin araştırıldığı çalışmalara olan ihtiyacı arttırmaktadır (Çetinkaya, Güldüren ve Keser, 2017). Araştırma bulgularının bu anlamda alan yazına katkı sağlaması beklenmektedir. Bu araştırmada; üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin belirlenmesi; eğitim fakültelerinin farklı programlarına devam eden öğrencilerle diğer fakülte öğrencilerinin siber güvenlik farkındalıklarının karşılaştırılması, farkındalık düzeyleri ile cinsiyet, sınıf

düzeyi, günlük akıllı telefon kullanım süresi değişkenleri arasında anlamlı bir farklılık olup olmadığının incelenmesi amaçlanmıştır. Bu amacın gerçekleşmesine yönelik olarak aşağıdaki sorulara cevap aranmıştır.

1. Üniversite öğrencilerinin siber güvenlik farkındalık düzeyi nedir?
2. Üniversite öğrencilerinin siber güvenlik farkındalık düzeyleri cinsiyet değişkenine göre anlamlı farklılık göstermekte midir?
3. Üniversite öğrencilerinin siber güvenlik farkındalık düzeyleri sınıf değişkenine göre anlamlı farklılık göstermekte midir?
4. Üniversite öğrencilerinin siber güvenlik farkındalık düzeyleri akıllı telefon kullanım sürelerine göre anlamlı bir şekilde farklılaşmakta mıdır?
5. Eğitim fakültesi öğrencilerinin siber güvenlik farkındalık düzeyleri ile diğer fakültelerdeki öğrencilerin farkındalık düzeyleri arasında anlamlı bir farklılık var mıdır?

YÖNTEM

Araştırmanın bu bölümünde araştırma modeli, çalışma grubu, veri toplama aracı ile verilerin analizine ilişkin bilgilere yer verilmiştir.

Araştırma Modeli

Nicel veri toplama tekniklerinin kullanıldığı bu araştırma genel tarama modellerinden tekil tarama modeli kullanılarak gerçekleştirilmiştir. Tekil tarama modelinde ilgilenilen konuya ilişkin olarak katılımcıların görüşlerinin veya ilgi, beceri, tutum gibi özellikleri ayrı ayrı betimlenmeye çalışılmaktadır (Karasar, 2009).

Çalışma grubu

Araştırmanın çalışma grubunu 2018-2019 eğitim-öğretim yılında üç farklı devlet üniversitesinde öğrenime devam eden ve gönüllülük esasına göre araştırmaya katılan 448 öğrenci oluşturmuştur. Öğrencilerin çalışma grubuna seçilmesinde seçkisiz olmayan örnekleme yöntemlerinden "*uygun örnekleme yöntemi*" seçilmiştir (Büyüköztürk, 2012). Bu örnekleme yönteminin seçilmesinde zaman, para ve işgücü unsurları gözönünde bulundurularak örneklemin kolay ulaşılabilir ve uygulama yapılabilir olması etkin olmuştur (Karasar, 2009). Katılımcıların demografik özelliklerine ilişkin betimsel istatistikler Tablo 1'de belirtilmiştir.

Tablo 1. Katılımcıların demografik özelliklerine ilişkin frekans ve yüzde dağılımları

Cinsiyet	N	%
Kadın	278	62.1
Erkek	170	37.9
Sınıf Düzeyi		
1.Sınıf	45	10.0
2.Sınıf	98	21.9
3.Sınıf	127	28.3
4.Sınıf	178	39.7
Günlük internet kullanım süresi		
≥ 2 saat	84	18.8
3-4 saat	140	31.3
5-6 saat	97	21.7
7 ≥ saat	127	28.3
Fakülte		
Eğitim Fakültesi öğrencisi	188	42.0
Diğer Fakülte öğrencisi	260	58.0
Toplam	448	100

Çalışma grubunda yer alan öğrencilerin %62'si (278) kadın, %38'i (170) erkek, en düşük yaş 18, en yüksek yaş 42 ve yaş ortalaması 22'dir. Katılımcıların tamamının akıllı telefon sahibi olduğu, %92'sinin internet bağlantısını akıllı telefonundan, %17'sinin dizüstü bilgisayarlarından ve %6'sının tablet bilgisayarlarından sağladığı anlaşılmıştır. Katılımcıların günlük ortalama internet kullanım süresinin 6 saate yakın olduğu anlaşılmıştır. Çalışma grubunda yer alan öğrencilerin öğrenim gördükleri lisans programlarını gösterir bilgiler Tablo 2'de sunulmuştur.

Tablo 2. Katılımcıların öğrenim gördükleri lisans programlarına ilişkin bilgiler

Eğitim Fakültesi Programları	N	%	Diğer Fakültelerin Programları	N	%
Arapça Öğretmenliği	25	5.6	Tarih	117	26.1
BÖTE	21	4.7	Fizik	17	3.8
Okul Öncesi Öğretmenliği	20	4.5	Sosyoloji	16	3.6
Müzik Öğretmenliği	18	4	Bilgisayar Mühendisliği	16	3.6
Tarih Öğretmenliği	17	3.8	Hukuk	13	2.9
Özel Eğitim Öğretmenliği	17	3.8	Kimya	11	2.5
İngilizce Öğretmenliği	16	3.6	Felsefe	10	2.2
Sınıf Öğretmenliği	16	3.6	Psikoloji	9	2
Sosyal Bilgiler Öğretmenliği	14	3.1	Biyoloji	8	1.8
Matematik Öğretmenliği	12	2.7	Makina Mühendisliği	5	1.1
Fen Bilgisi Öğretmenliği	11	2.5	Fizik Tedavi ve Rehabilitasyon	1	.2
Türkçe Öğretmenliği	8	1.8			
Resim İş Öğretmenliği	8	1.8			
Kimya Öğretmenliği	6	1.3			
Almanca Öğretmenliği	5	1.1			
Rehberlik ve Psik. Danışmanlık	5	1.1			
Fizik Öğretmenliği	4	.9			
Beden Eğitimi Öğretmenliği	2	.4			
Toplam	188	42		260	58

Tablo 2'de görüleceği üzere öğrencilerin 188'inin eğitim fakültelerindeki farklı öğretmenlik lisans programlarına devam ettiği, 260'ının da öğretmenlik programları dışındaki fakültelerde öğrenime devam ettiği anlaşılmıştır.

Veri Toplama Aracı

Araştırmada katılımcıların demografik özellikleri, yaş, cinsiyet, öğrenim gördükleri üniversite, bölüm, sınıf düzeyi ve günlük internet kullanım süresi bilgileri araştırmacı tarafından geliştirilen anket formuyla toplanmıştır. Kişisel siber güvenlik farkındalıklarının belirlenmesi amacıyla Erol, Şahin, Yılmaz ve Haseki (2015) tarafından geliştirilen *Kişisel Siber Güvenliği Sağlama Ölçeği (KSGSÖ)* kullanılmıştır. Hiçbir zaman katılmıyorum (1), Her zaman katılıyorum (5) şeklinde puanlanan 5'li likert türü 25 maddeden oluşan ölçek, (*1) Kişisel gizliliği koruma, (2) Güvenilmeyenden kaçınma, (3) Önlem alma, (4) Ödeme bilgilerini koruma ve (5) İz bırakmama* olmak üzere 5 faktörden oluşmuştur. Çalışmada ölçeğin Cronbach Alfa güvenirlik katsayısı 0.804 olarak bulunmuştur. Ölçeğin *"kişisel güvenliği koruma"* faktörü güvenirlik katsayısı 0.745, "*güvenilmeyenden kaçınma"* faktörü güvenirlik katsayısı 0.737, *"önlem alma"* faktörü güvenirlik katsayısı 0.739, *"ödeme bilgilerini koruma"* faktörü güvenirlik katsayısı 0.786 ve *"iz bırakmama"* faktörü güvenirlik katsayısı 0.506 olarak bulunmuştur.

Verilerinin Analizi

Verilerin toplanması amacıyla basılı ve elektronik ortamda olmak üzere iki farklı biçimde veri toplama aracı hazırlanmıştır. Basılı formların sınıf ortamında doldurulması sağlanırken, ölçeğin elektronik formu için üç üniversitenin ulaşılabilen öğrenci gruplarına veri toplama aracına ilişkin bağlantı gönderilerek doldurulması talep edilmiştir. Doldurulan ölçme araçlarının yapılan ön değerlendirmesinde eksik ve hatalı kodlama yapılanlar değerlendirme dışı tutulmuştur. 448 katılımcıdan elde edilen veriler SPSS 23.0 istatistik programına aktarılarak analiz edilmiştir.

Analiz sürecinde kullanılacak istatistiksel testlerin belirlenmesi amacıyla faktörlerin basıklık ve çarpıklık katsayıları hesaplanmıştır. Çarpıklık katsayısı -0.452, basıklık katsayısı 1.787 bulunmuştur. Çarpıklık ve basıklık katsayılarının -2 ile +2 arasında olması ölçek puanlarının normal dağılımı açısından kabul edilebilir sınırlar olarak değerlendirildiği görülmektedir (George ve Mallery, 2010). Levene testi sonuçlarının varyansların homojenliği ve normal dağılım sağladığını göstermesi üzerine t-testi, tek yönlü varyans analizi (ANOVA) ve bağımlı değişken sayısının birden fazla olduğu durumlarda çok değişkenli ANOVA (MANOVA) uygulanmıştır. KSGSÖ puan aralıklarının belirlenmesinde, Yenilmez (2008) tarafından yapılan; Hiçbir zaman (1.0-1.80), Nadiren (1.81-2.60), Ara sıra (2.61-3.40), Sık sık (3.41-4.20), Her zaman (4.21-5.0) şeklindeki sınıflandırma dikkate alınmıştır. Ortalamalar arasındaki farkın anlamlılığını yorumlamada, Cohen (1998) tarafından belirlenen etki düzeyi kriterleri esas alınmıştır. Buna göre, Kısmi eta kare (η^2) 0.01 düzeyi düşük etki,

kısmi eta kare (η^2) 0.06 düzeyi orta etki ve kısmi eta kare (η^2) 0.14 düzeyi yüksek etki olarak yorumlanmıştır.

BULGULAR

Araştırmanın bu bölümünde araştırma amacı çerçevesinde veri toplama araçlarından elde edilen bulgulara yer verilmiştir.

Öğrencilerin siber güvenlik farkındalık düzeyleri

Öğrencilerin siber güvenlik farkındalık düzeylerinin ölçek alt faktörlerine göre incelendiği ortalama ve standart sapma değerleri Tablo 3'de belirtilmiştir.

Tablo 3. KSGSÖ faktörlerine ilişkin ortalama puanlar ve standart sapma değerleri

Faktör	Minimum	Maksimum	Ortalama	Standart Sapma
Kişisel Gizliliği Koruma	1	5	2.78	.73
Güvenilmeyenden Kaçınma	1	5	3.86	.95
Önlem Alma	1	5	3.37	.87
Ödeme Bilgilerini Koruma	1	5	3.70	1.16
İz Bırakmama	1	5	3.53	.80
Siber Güvenliği Sağlama Ölçeği	1	5	3.26	.57

Kişisel siber güvenliği sağlama ölçeği ve alt faktörlerine ilişkin ortalama puanlar ve standart sapma değerlerinin verildiği Tablo 3 incelendiğinde, en yüksek ortalama puanın "*güvenilmeyenden kaçınma"* ($\bar{X}$=3.86, SS=.95), faktöründe, en düşük ortalama puanın "*kişisel gizliliği koruma*" ($\bar{X}$=2.78, SS=.73) faktöründe alındığı görülmektedir. Ölçeğin tamamına ilişkin ortalama puanlar incelendiğinde ($\bar{X}$=3.26, SS=.57) öğrencilerin siber güvenlikle ilgili maddelere ölçekteki "Ara sıra" (2.61-3.40) sınırları içerisinde kalan orta farkındalık düzeyinin üst sınırına yakın düzeyde olduğu anlaşılmıştır.

Öğrencilerin siber güvenlik farkındalıklarının cinsiyete göre karşılaştırılması

Üniversite öğrencilerin siber güvenlik farkındalık düzeylerinin cinsiyet değişkenine göre anlamlı farklılık gösterip göstermediği bağımsız örneklem t-testi ile incelenmiştir.

Tablo 4. Siber güvenlik farkındalığının cinsiyete göre karşılaştırılması

Cinsiyet	N	Ortalama	Standart Sapma	*t*	df	p
Kadın	278	3.26	.521	.236	446	.81
Erkek	170	3.25	.573			

Öğrencilerin siber güvenlik farkındalık düzeylerinin cinsiyet değişkenine göre anlamlı farklılık gösterip göstermediğinin incelendiği t-testi sonuçları [$t_{(446)}$ =.236, p>.05] siber güvenlik farkındalığı ile cinsiyet arasında anlamlı bir farklılık bulunmadığını göstermiştir. Diğer taraftan, fakülte durumuna göre öğrencilerin siber güvenlik farkındalık düzeyleri ile cinsiyet arasında anlamlı bir farklılık bulunup bulunmadığı da bağımsız örneklem t-testi ile incelenmiş ve sonuçlar Tablo 5'de verilmiştir.

Tablo 5. Siber güvenlik farkındalığının cinsiyete ve fakülte durumuna göre karşılaştırılması

Fakülte	Cinsiyet	N	Ortalama	Standart Sapma	*t*	df	p
Eğitim Fakültesi	Kadın	129	3.29	.399	-.175	186	.86
	Erkek	59	3.30	.391			
Diğer Fakülteler	Kadın	149	3.24	.60	.185	258	.85
	Erkek	111	3.22	.65			

p<0.05

Tablo 5 incelendiğinde; eğitim fakültesi öğrencilerinin siber güvenlik farkındalıklarının cinsiyet değişkenine göre anlamlı farklılık göstermediği [$t_{(186)}$ =-.175, $p>.05$] sonucuna ulaşılmıştır. Benzer şekilde, diğer bazı fakültelerde öğrenime devam eden öğrencilerin siber güvenlik farkındalıkları ile cinsiyet arasında da anlamlı bir farklılık [$t_{(258)}$ =.185, $p>.05$] bulunmamıştır.

Öğrencilerin siber güvenlik farkındalıklarının sınıf düzeyine göre karşılaştırılması

Üniversite öğrencilerinin siber güvenlik farkındalıkları ile sınıf düzeyi arasındaki ilişki MANOVA testi uygulanarak analiz edilmiş, sonuçlar Tablo 6'da verilmiştir.

Tablo 6. Siber güvenlik farkındalıklarının sınıf düzeyine göre karşılaştırılması

		Kişisel Gizlilik Koruma		Güvenil-meyenden Kaçınma		Önlem Alma		Ödeme Bilgilerini Koruma		İz Bırakmama		F (3,444)	p	kısmi η^2
Sınıf	N	$\bar{X}$	SS	$\bar{X}$	SS	$\bar{X}$	SS	$\bar{X}$	SS	$\bar{X}$	SS			
1. Sınıf	45	2.89	.10	4.10	.14	3.47	.12	3.80	.17	3.73	.11	2.78	.00	.03
2. Sınıf	98	2.92	.07	3.57	.09	3.24	.08	3.42	.11	3.20	.07			
3. Sınıf	127	2.64	.06	3.97	.08	3.35	.07	3.87	.10	3.63	.07			
4. Sınıf	178	2.77	.05	3.86	.07	3.41	.06	3.70	.08	3.58	.05			

Öğrencilerin siber güvenlik farkındalıklarının sınıf düzeyine göre incelendiği MANOVA sonuçları [$F_{(3,444)}$=2.78, p<.05; Wilk's λ=.911, kısmi η^2=.03] üniversite öğrencilerinin siber güvenlik farkındalıkları ile sınıf düzeyleri arasında anlamlı farklılık olduğunu ortaya koymuştur. Farkın kaynağını bulmak amacıyla gerçekleştirilen Scheffe testi sonuçları, *kişisel gizliliği koruma* alt faktöründe [$F_{(3,444)}$=3.132, p<.05; kısmi η^2=.02] 2.sınıfların ortalama puanları ile 3.sınıfların ortalama puanları arasında 2.sınıflar lehine etki büyüklüğü düşük düzeyde anlamlı farklılık olduğunu göstermiştir. *İz bırakmama* faktöründe [$F_{(3-444)}$=7.682, p<.05; kısmi η^2=.04] 1.sınıflarla 2.sınıflar arasında 1.sınıflar lehine, 3.sınıflarla 2.sınıflar arasında 3.sınıflar lehine, 4.sınıflarla 2.sınıflar arasında 4.sınıflar lehine düşük düzeyde anlamlı farklılık olduğu anlaşılmıştır. *Ödeme bilgilerini koruma* faktöründe 3.sınıflarla 2.sınıflar arasında 3.sınıflar lehine etki büyüklüğü düşük düzeyde anlamlı farklılık bulunmuştur. *Güvenilmeyenden kaçınma* faktöründe ise 1.sınıflarla 2.sınıflar arasında 1.sınıflar lehine, 2.sınıflarla 3.sınıflar lehine düşük etki büyüklüğünde (kısmi η^2=.03) anlamlı farklılık bulunduğu, diğer sınıf düzeyleri arasında ise anlamlı bir farklılık bulunmadığı sonucuna ulaşılmıştır. *Önlem alma* alt faktöründe ise sınıflar arası anlamlı bir farklılık bulunmamıştır.

Öğrencilerinin siber güvenlik farkındalıklarının öğrenim gördükleri fakülte durumu ve sınıf düzeyi değişkenleri açısından incelenmesine ilişkin puan ortalamaları ve tek yönlü varyans analizi (ANOVA) sonuçları Tablo 7'de verilmiştir.

Tablo 7. Siber güvenlik farkındalıklarının fakülte ve sınıf düzeyine göre karşılaştırılması

Fakülte	Sınıf	*N*	$\bar{X}$	*Ss*	VK	KT	Sd	KO	*F*	*p*
Eğitim Fakültesi	1	16	3.32	.462	Grup.Arası	.20	3	.70	.439	.72
	2	4	3.44	.195	Grup. içi	29.15	184	.15		
	3	80	3.32	.347	Toplam	29.36	187			
	4	88	3.27	.432						
Diğer Fakülteler	1	29	3.45	.625	Grup.Arası	2.58	3	.86	2.234	.08
	2	94	3.16	.660	Grup. içi	98.59	256	.38		
	3	47	3.13	.678	Toplam	101.17	259			
	4	90	3.28	.539						

p>.05

Üniversite öğrencilerinin siber güvenlik farkındalıklarının fakülte durumu ve sınıf düzeyine göre incelenmesine ilişkin bulgular Tablo 7'de görülmektedir. Buna göre, eğitim fakültesi öğrencileri ($F_{(3,184)}$=.439; p<.05) ile diğer programlara devam eden öğrencilerin sınıf düzeyleri ve siber güvenlik farkındalıkları ($F_{(3,256)}$=2.234; p<.05) arasında anlamlı bir farklılık bulunmamıştır.

Öğrencilerin siber güvenlik farkındalık düzeylerinin günlük internet kullanım süresine göre incelenmesi

Üniversite öğrencilerinin siber güvenlik farkındalıklarının günlük internet kullanım sürelerine göre incelenmesine ilişkin ortalama ve standart sapma değerleri Tablo 8'de verilmiştir.

Tablo 8. Siber güvenlik farkındalıklarının internet kullanım sürelerine göre incelenmesi

		Kişisel Gizlilik Koruma		Güvenilm. Kaçınma		Önlem Alma		Ödeme Bilgilerini Koruma		İz Bırakma ma		F (3,444)	p	kısmi η^2
GİKSüre	N	$\bar{X}$	SS	$\bar{X}$	SS	$\bar{X}$	SS	$\bar{X}$	SS	$\bar{X}$	SS			
≥ 2 saat	84	2.55	.72	3.86	1.08	3.25	.88	3.66	1.27	3.47	.95	3.742	.00	.04
3-4 saat	140	2.66	.65	3.88	.95	3.23	.87	3.71	1.17	3.50	.77			
5-6 saat	97	2.77	.67	3.90	.93	3.28	.78	3.69	1.15	3.41	.80			
7 ≥ saat	127	3.04	.80	3.77	.87	3.65	.84	3.71	1.07	3.69	.69			

Öğrencilerin siber güvenlik farkındalıklarının günlük akıllı telefon kullanım sürelerine göre anlamlı bir şekilde farklılaşıp farklılaşmadığı MANOVA testi ile incelenmiştir. MANOVA testi sonuçları [$F_{(3,444)}$=3.742, p<.05; Wilk's λ=.883, kısmi eta-kare η^2=.04] öğrencilerin siber güvenlik farkındalıkları ile internet kullanım süreleri arasında anlamlı bir farklılık bulunduğunu göstermiştir. Farklılığın kaynağını belirlemek amacıyla gerçekleştirilen Scheffe testi sonuçları, *kişisel gizliliği*

koruma alt faktöründe günlük 2 saatten az internet kullanan öğrenciler ($\bar{X} = 2.55$) ile 7 saatten fazla kullanan ($\bar{X} = 3.04$) öğrenciler arasında 7 saatten fazla kullananlar lehine anlamlı bir farklılık bulunduğunu göstermiştir. Cohen (1988) kriterlerine göre ortalama farklarının etki büyüklüğünün orta düzeyde (kısmi eta-kare η^2=.06) olduğu anlaşılmıştır. *Önlem alma* faktöründe, Tablo 8'de görüleceği üzere günlük 7 saatten fazla internet kullanan öğrencilerin ortalamaları ile diğer günlük internet kullanım ortalamaları arasında 7 saatten fazla kullananlar lehine etki büyüklüğü düşük düzeyde (kısmi eta-kare η^2=.04) anlamlı bir farklılık bulunduğu sonucuna ulaşılmıştır. *İz bırakmama, ödeme bilgilerini koruma* ve *güvenilmeyenden kaçınma* alt faktörlerinde ise öğrencilerin siber güvenlik farkındalıkları ile günlük internet kullanım süreleri arasında anlamlı bir farklılık bulunmamıştır.

Öğrencilerinin siber güvenlik farkındalık düzeylerinin fakülte durumuna göre karşılaştırılması

Eğitim fakültelerinin farklı programlarında öğrenim gören öğrencilerle diğer bazı fakültelerde öğrenim gören öğrencilerin siber güvenlik farkındalık düzeyleri bağımsız örneklem t-testi ile incelenmiş, sonuçlar Tablo 9'da sunulmuştur.

Tablo 9. Siber güvenlik farkındalığının fakülte durumuna göre karşılaştırılması

Fakülte	N	Ortalama	Standart Sapma	*t*	*df*	*p*
Eğitim Fakültesi	188	3.30	.396	1.378	446	.16
Diğer Fakülteler	260	3.23	.625			

Tablo 9 incelendiğinde; eğitim fakültesi öğrencilerinin siber güvenlik farkındalık düzeyleri ile diğer bazı fakültelerde öğrenim gören öğrencilerin siber güvenlik farkındalık düzeyleri arasında [$t_{(446)}$ = 1.378, p>.05] anlamlı farklılık bulunmadığı sonucuna ulaşılmıştır.

TARTIŞMA, SONUÇ VE ÖNERİLER

Bu araştırmada; üniversite öğrencilerinin siber güvenlik farkındalık düzeylerinin belirlenmesi; farkındalık düzeyleri ile cinsiyet, sınıf düzeyi, günlük akıllı telefon kullanım süresi ve fakülte değişkenleri arasında anlamlı bir farklılık bulunup bulunmadığı incelenmiştir. Araştırma bulguları Tablo 10'da özetlenmiştir.

Tablo 10. Araştırma bulguları özeti

		KGK	**GK**	**ÖA**	**ÖBK**	**İB**
Siber güvenlik farkındalığı		Orta Düzey	İyi Düzey	Orta düzey	İyi Düzey	İyi düzey
Cinsiyet		-	-	-	-	-
Sınıf düzeyi	1=1.Sınıf 2=2.Sınıf 3=3.Sınıf 4=4.Sınıf	2>3 *	1>2* 3>2*		3>2*	1>2* 3>2* 4>2*
Fakülte Türü-Sınıf Düzeyi		-	-	-	-	-
Günlük İnternet Kullanım Süresi	1= ≥ 2 saat 2= 3-4 saat 3= 5-6 saat 4= 7 ≥ saat	4>1**	-	4>3* 4>2* 4>1*	-	-
Siber Güvenlik Farkındalığı-Eğitim Fakültesi/Diğer Fak.		-	-	-	-	-

Orta düzey: Ölçekteki 3-Ara sıra (2.61-3.40) aralığındaki puanlar *KGK: Kişisel Gizliliği Koruma*
İyi düzey: Ölçekteki 4-Sık sık (3.41-4.20) aralığındaki puanlar *GK: Güvenilmeyenden Kaçınma*
** Düşük etki büyüklüğünde (Kısmi eta kare (η^2) 0.01 düzeyi) anlamlı fark* *ÖA: Önlem Alma İB: İz Bırakmama*
*** Orta etki büyüklüğünde (Kısmi eta kare (η^2) 0.06 düzeyi) anlamlı fark* *ÖBK: Ödeme Bilgilerine Koruma*

Araştırma bulguları, öğrencilerin siber güvenlik farkındalıklarının *güvenilmeyenden kaçınma, ödeme bilgilerini koruma* ve *iz bırakmama* faktörlerinde yeterli ve iyi düzey olarak kabul edilen 3.41-4.20 (Yenilmez, 2008) aralığında, ölçeğin tamamında da ortanın üst sınırına yakın düzeyde olduğunu göstermiştir. Öğrencilerin en yüksek ortalamaya; *internet üzerinden yapılan para ve kontör gibi talepleri dikkate almama, tanımadığı kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmeme, güvenli olmayan sitelere üye olmama ve dosya indirmeme* gibi ölçek maddelerinin yer aldığı "*güvenilmeyenden kaçınma"* faktöründe ulaştıkları görülmüştür. Sosyal mühendislik ve oltalama gibi yöntemler kullanılarak gerçekleştirilen siber saldırıların yoğunluğu göz önünde bulundurulduğunda öğrencilerin siber güvenlik farkındalık düzeylerine ilişkin bu sonuç oldukça önemli bulunmuştur.

Öğrencilerin siber güvenlik farkındalıklarına ilişkin en düşük ortalamaya, internet şifrelerinin tümünün aynı olması, e-postalarla gelen kimlik doğrulama mesajlarını cevaplama, tanımadığı kişilerden gelen e-postaları açma ve akılda kalıcılık açısından kolay şifre belirleme gibi maddelerin yer aldığı "kişisel gizliliği koruma" alt faktöründe ulaşılmıştır. Bu sonucun, Yılmaz ve diğerleri (2016) tarafından vurgulanan bireysel ya da kurumsal kullanıcıların önceden gerekli önlemleri almak yerine ciddi bir sorunla karşılaştıkları zaman harekete geçme eğiliminde oldukları yönündeki görüşü doğrular nitelikte olduğu değerlendirilmektedir. Şifre güvenliği, e-posta güvenliği, kişisel bilgilerin güvenliği gibi kullanıcıların sorumluluğunda olan maddelerin yer aldığı bu faktöre ilişkin puan ortalamasının araştırmada ulaşılan en düşük puan ortalaması olması, siber güvenlikte en zayıf halkanın insan unsuru olduğu gerçeğinin bir yansıması olarak yorumlanabilir. Bu sonuç, öğrencilerin siber güvenlik farkındalıklarının arttırılmasına yönelik eğitim ihtiyacının bir göstergesi olarak da değerlendirilebilir.

Bu araştırmanın öğrencilerin siber güvenlik farkındalık düzeylerine ilişkin bulgularına benzer şekilde, Rani (2017) tarafından gerçekleştirilen çalışmada siber güvenlik farkındalıklarının orta

düzeyde olduğu görülmüştür. Akgün ve Topal (2015) tarafından gerçekleştirilen çalışmada benzer sonuçlara ulaşılmış, katılımcıların farkındalık düzeyleri genel itibariyle yeterli bulunmakla birlikte azımsanamayacak sayıda öğrencinin farkındalık düzeylerinin yeterli düzeyin altında kaldığı anlaşılmıştır. Alan yazında, üniversite öğrencilerinin siber güvenlik farkındalıklarının yeterli düzeyde olduğunu gösteren araştırmalar bulunmaktadır (Karacı vd., 2017; Yiğit ve Seferoğlu, 2019). Bu araştırma bulgularından farklı olarak öğrencilerin siber güvenlik davranışlarının yetersiz olduğu sonucuna ulaşılan çok sayıda araştırma olduğu görülmektedir (Bulu vd., 2017; Gökmen ve Akgün, 2016; Karaoğlan Yılmaz vd., 2014; Kaşıkcı, Çağıltay, Karakuş, Kurşun ve Ogan, 2014; Pusey ve Sadera, 2011; Tekerek ve Tekerek, 2013). Konuya ilişkin olarak yapılmış çalışmaların büyük bölümünde katılımcıların siber güvenlik farkındalıklarının yeterli bulunmadığı ve farkındalık düzeylerinin arttırılmasına yönelik eğitim faaliyetlerine ihtiyaç duyulduğu vurgusu yapılmıştır.

Üniversite öğrencilerinin siber güvenlik farkındalıklarının cinsiyet değişkenine göre farklılaşıp farklılaşmadığına ilişkin bulgular, kadın öğrencilerle erkek öğrenciler arasında anlamlı düzeyde bir farklılık bulunmadığını göstermiştir. Benzer şekilde alan yazında, siber güvenlik farkındalık düzeyi ile cinsiyet arasında anlamlı farklılık bulunmadığını gösteren araştırmalar bulunmaktadır (Karacı vd., 2017; Mart, 2012; Rani, 2017; Yiğit ve Seferoğlu, 2019). Bu bulgulardan farklı olarak, bazı araştırmalarda erkeklerin siber güvenlik farkındalıklarının kadınlara oranla daha yüksek olduğu sonucuna ulaşılmıştır (Güldüren, Çetinkaya ve Keser, 2016; Yılmaz vd., 2016). Bu araştırmada ayrıca, eğitim fakültesi ve diğer bazı fakültelerdeki öğrencilerin siber güvenlik farkındalık düzeyleri ile cinsiyet arasında anlamlı farklılık bulunmadığı görülmüştür.

Araştırmada öğrencilerin siber güvenlik farkındalık düzeyleri ile sınıf düzeyleri arasında anlamlı farklılık bulunduğu sonucuna ulaşılmıştır. *Kişisel gizliliği koruma* faktöründe 2.sınıflarla 3.sınıflar arasında 2. Sınıflar lehine düşük etki düzeyinde anlamlı fark bulunurken, *iz bırakmama* faktöründe 1.sınıfların 2.sınıflara göre, 3.sınıfların 2.sınıflara göre, 4.sınıfların 2.sınıflara göre düşük etki düzeyinde anlamlı farklılık bulunmuştur. Bu sonuçlar, 2.sınıf öğrencilerinin *iz bırakmama* davranışı sergilemeye yönelik farkındalıklarının en düşük düzeyde olduğunu göstermiştir. *Ödeme bilgilerini koruma* faktöründe 3.sınıfların 2.sınıflara oranla düşük etki düzeyinde anlamlı farklılık bulunduğu, bu faktöre ilişkin diğer sınıf düzeyleri arasında ise anlamlı bir farklılık bulunmadığı sonucuna ulaşılmıştır. *Güvenilmeyenden kaçınma* faktörüne ilişkin bulgular, 1.sınıf ve 3.sınıf öğrencilerinin 2.sınıflara kıyasla düşük etki düzeyinde anlamlı farklılık olduğu görülmüş, diğer sınıf düzeyleri arasında anlamlı farklılık bulunmamıştır. *Önlem alma* faktöründe sınıflar arası anlamlı bir farklılık bulunmadığı anlaşılmaktadır. Üniversite öğrencilerinin siber güvenlik farkındalıklarının fakülte ve sınıf düzeyine göre incelenmesine ilişkin bulgular bu iki grup arasında anlamlı farklılık bulunmadığını ortaya koymuştur.

Araştırmanın sınıf düzeyine ilişkin bulguları alan yazında üniversite öğrencilerinin siber güvenlik farkındalık düzeyleri ile sınıf düzeylerinin incelendiği bazı araştırma bulgularıyla farklılık göstermektedir. Yiğit ve Seferoğlu (2019) tarafından gerçekleştirilen araştırmada öğrencilerin siber güvenlik davranışları ile sınıf düzeyleri arasında anlamlı farklılıkların bulunduğu sonucuna ulaşılmıştır. Bu çalışmada, ön lisans öğrencilerinin siber güvenlik davranışları en düşük düzeyde, 4.sınıf öğrencilerinin siber güvenlik davranışları ise en yüksek düzeyde bulunmuş, öğrencilerin sınıf düzeyiyle doğru orantılı olarak siber güvenlik davranış düzeylerinin de arttığı sonucuna ulaşılmıştır. Benzer sonuçlara, Tekerek ve Tekerek (2013) tarafından ilköğretim ve lise öğrencileri ile gerçekleştirilen araştırmada ulaşılmış, sınıf düzeyinin artışıyla birlikte öğrencilerin bilgi güvenliği farkındalıklarının arttığı görülmüştür. Bu bulgulardan farklı olarak, Karacı ve diğerleri (2017) tarafından gerçekleştirilen araştırmada üniversite öğrencilerinin sınıf düzeyi ile siber güvenlik farkındalıkları arasında anlamlı bir farklılık bulunmadığı sonucuna ulaşılmıştır.

Akıllı telefonların yaygın olarak kullanılmasıyla birlikte siber güvenlikle ilgili tehdit ve tehlikeler farklılaşarak artmaya devam etmektedir. Öğrencilerin siber güvenlik davranışları ile günlük internet kullanım süreleri arasındaki ilişki bu çerçevede araştırmaya konu edilmiştir. Araştırma bulguları, öğrencilerin siber güvenlik farkındalık düzeyleri ile günlük akıllı telefon kullanım süreleri arasında orta etki düzeyinde anlamlı farklılık bulunduğunu göstermiştir. Bulgular, *kişisel gizliliği koruma* faktöründe günlük 2 saatten az internet kullanan öğrenciler ile 7 saatten fazla kullananlar arasında orta etki düzeyinde anlamlı farklılık olduğunu ortaya koymuştur. Önlem *alma* faktöründe, 7 saatten fazla internet kullananlarla diğer tüm kullanım düzeyleri arasında orta etki büyüklüğünde anlamlı farklılık bulunmuştur. Öğrencilerin siber güvenlik farkındalık düzeylerinin *iz bırakmama, ödeme bilgilerini koruma* ve g*üvenilmeyenden kaçınma* faktörlerinde günlük internet kullanım sürelerine göre anlamlı şekilde farklılaşmadığı sonucuna ulaşılmıştır. Yılmaz ve diğerleri (2016) tarafından gerçekleştirilen çalışmada da, günlük internet kullanım süresi ile dijital veri güvenliği sağlama davranışları arasında anlamlı farklılık bulunduğu sonucuna ulaşılmıştır. Bu bulgulardan farklı olarak öğrencilerin siber güvenlik davranış düzeyleri ile internet kullanım süreleri arasında anlamlı ilişki bulunmadığı sonucuna ulaşılan çalışmalar bulunmaktadır (Akgün ve Topal, 2015; Gökmen ve Akgün, 2016; Yiğit ve Seferoğlu, 2019). Ulaşılan farklı sonuçlar, siber güvenlik risklerinin artarak devam etmesi ve etkilerinin daha yıkıcı sonuçlar ortaya çıkarma potansiyeli bu tür çalışmaların yapılmaya devam edilmesi gerektiği şeklinde yorumlanabilir.

Araştırma bulguları, eğitim fakültesi öğrencilerinin siber güvenlik farkındalık düzeyleri ile diğer bazı fakültelerdeki öğrencilerin siber güvenlik farkındalık düzeyleri arasında anlamlı farklılık bulunmadığını ortaya koymuştur. Bu durum, mezuniyetleri sonrası kendilerinden öğrencilerine siber güvenlik farkındalığı kazandırmaları beklenen öğretmen adayları açısından son derece dikkate değer bulunmuştur. Eğitim fakültelerinde öğrenim gören öğretmen adaylarının siber güvenlik

farkındalıklarının yüksek olması sadece kişisel güvenlikleri açısından değil, meslek yaşamlarında kullanmak zorunda oldukları MEBBİS, e-Okul, EBA gibi çok sayıda kurumsal elektronik sistemin güvenliği açısından önem taşımaktadır. İçinde bulunduğumuz çağın gerekleri göz önünde bulundurulduğunda öğrencilere siber güvenlik farkındalığı kazandırma sadece bilişim teknolojisi öğretmenlerinin sorumluluğunda olmaktan çıktığı düşünülmektedir. Bu çerçevede, tüm öğretmenlerin öğrencilerini siber ortamlardaki tehdit ve tehlikeler konusunda bilgilendirmeleri ve rol model olmaları beklenmektedir. Bu sorumlulukların yerine getirilmesi ve beklentilerin karşılanması öğretmen adaylarının yeterli bilgi, beceri ve davranışlar kazanmış olarak mezun olmalarını gerekmektedir. Bu konuda yükseköğretim kurumlarının programlarını alandaki gelişmeler doğrultusunda güncellemeleri ve farkındalık kazandırmaya yönelik faaliyetlere yer vermeleri gerekmektedir.

Mevcut araştırma bulgularından anlaşılacağı üzere, üniversite öğrencilerin farkındalık düzeyinin ölçeğin bazı alt faktörlerinde yeterli olmasına rağmen, kişisel siber güvenliğin sağlanması açısından kritik önem taşıyan bazı faktörlerde orta düzeyde kalması, öğrencilerin siber güvenlik farkındalıklarının artırılmasına yönelik eğitimlere ihtiyaç duyulduğu şeklinde yorumlanabilir. Bilişim güvenliği eğitimi almış olmakla birlikte öğrencilerin siber güvenlik farkındalığı açısından istenilen düzeyde olmadığını gösteren araştırmalar yanında (Akgün ve Topal, 2015), bilişim güvenliği eğitimi almış olmanın siber güvenlik farkındalık ve davranışlarını olumlu etkilediği sonucuna ulaşılan araştırmalar bulunmaktadır (Yiğit ve Seferoğlu, 2019). Alan yazında siber güvenlik eğitimlerinin siber güvenlik davranışları üzerindeki etkililiğine ilişkin farklı sonuçların bu eğitimlerin içeriği, eğiticileri ve eğitimin niteliğinden kaynaklanabileceği değerlendirilmektedir. Siber güvenlikle ilgili eğitimlerin öğrencilerin bilgi ve beceri seviyelerine göre güncel, öğrenen odaklı, tutum ve davranış kazandırmaya yönelik olarak planlanması ve eğitimlerin etkililiğinin değerlendirilmesi önerilmektedir.

Araştırma bulgularının alan yazına katkı sağlaması ve gelecekte yapılacak benzer çalışmalara ışık tutması beklenmektedir. Bununla birlikte, araştırmanın temel bazı sınırlılıkları bulunmaktadır. Araştırma evreninin üç devlet üniversitesi öğrencileriyle sınırlı tutulması ve çalışma grubunun uygun örneklem yöntemiyle belirlenmiş olması araştırmanın genellenebilirliği açısından sınırlılık olarak görülmektedir. Gelecek çalışmalarda sonuçların genellenebilirliği açısından devlet ve özel üniversitelerden araştırma evrenini temsil edecek gruplar üzerinde araştırmalar gerçekleştirilebilir.

KAYNAKÇA

Akgün, Ö.E. & Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi eğitim fakültesi örneği. *Sakarya Üniversitesi Eğitim Fakültesi Dergisi, 5*(2), 98-121.

Bıçakcı, S., Ergun, D. & Çelikpala, M. (2015). *Türkiye'de siber güvenlik*. EDAM Siber Güvenlik Kağıtları Serisi 2015/1.

Bilgiç, H.G., Duman, D. & Seferoğlu, S.S. (2011). Dijital yerlilerin özellikleri ve çevrim içi ortamların tasarlanmasındaki etkileri. *Akademik Bilişim'11 - XIII. Akademik Bilişim Konferansı Bildirileri,* 2 - 4 Şubat 2011 İnönü Üniversitesi, Malatya.

Brar, H. S. & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications, 1*-11.

Bulu, Ş., Kavuk, M., & Keser, H. (2017). Pre-service ICT teachers' recommendations for school internet safety. *The Association for Educational Communications and Technology,* 1, 93-97.

Büyüközürk, Ş. (2012). Örnekleme yöntemleri. 23 Şubat 2019 tarihinde http://w3.balikesir. edu.tr/~msackes/wp/wp-content/uploads/2012/03/BAY-Final-Konulari.pdf adresinden erişilmiştir.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Erlbaum.

Çatak, P.D. & Ögel, K. (2010). Bir terapi yöntemi olarak farkındalık. *Nöropsikiyatri Arşivi, 47*, 69-73.

Çetinkaya, L., Güldüren, C. & Keser, H. (2017). Öğretmenler için bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *Milli Eğitim Dergisi, 216,* 33-52.

Çubukçu, A. & Bayram Ş. (2013). Türkiye'de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern & African Journal of Educational Research, 5*, 148-174.

Erdem, M. & Özocak, G. (2019). Siber güvenliğin sağlanmasında uluslararası hukukun ve Türk hukukunun rolü. *Ankara Üniversitesi Hukuk Fakültesi Dergisi, 68*(1), 127-212.

Erol, O., Şahin, Y.L., Yılmaz, E., & Haseski, H.İ. (2015). Kişisel siber güvenliği sağlama ölçeği geliştirme çalışması. *International Journal of Human Sciences, 12*(2), 75-91.

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

Farrukh, A., Sadwick, R. & Villasenor, J. (2014). *Youth Internet Safety: Risks, Responses, and Research Recommendations*. Center for Technology Innovation at Brookings: Washington.

George, D. & Mallery, M. (2010). *SPSS for Windows Step by Step: A Simple Guide and Reference, 17.0 update* (10a ed.) Boston: Pearson.

Gökmen, Ö.F. & Akgün, Ö.E. (2016). Öğretmen adaylarının bilişim suçlarına yönelik deneyimleri ve bilişim güvenliği ders içeriğine yönelik görüşleri. *Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 13*(33), 178-193.

Gönen, S., Ulus, H.İ. & Yılmaz, E.N. (2016). Bilişim alanında işlenen suçlar üzerine bir inceleme. *Bilişim Teknolojileri Dergisi, 9*(3), 229-236.

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

GüvenliWEB (2019). İnternette hak & hukuk ve sorumluluklar. 23 Nisan 2019 tarihinde https://www.guvenliweb.org.tr/dokuman-detay/internette-hak-hukuk-ve-sorumluluklar adresinden erişilmiştir.

Karacı, A., Akyüz, H. İ. & Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi, 25*(6), 2079-2094.

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

Karasar, N. (2009). *Bilimsel Araştırma Yöntemi*. (20. Baskı). Ankara: Nobel Yayın Dağıtım.

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

Kavuk, M., Keser, H. & Teker, N. (2011). Reviewing unethical behaviors of primary education students' internet usage. *Procedia-Social and Behavioral Sciences, 28*, 1043-1052.

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

Li, X. (2017). A Review of motivations of ıllegal cyber activities. *Criminology & Social Integration Journal, 25*(1), 110-126.

Mart, İ. (2012). *Bilişim Kültüründe Bilgi Güvenliği Farkındalığı*. Yüksek lisans tezi. Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Kahramanmaraş.

MEB (2019). FATİH projesi hakkında. 22 Haziran 2019 tarihinde http://fatihprojesi.meb.gov.tr/about.html adresinden erişilmiştir.

MEBBİS (2015). Millî Eğitim Bakanlığı bilişim sistemleri tanıtım videosu. 16 Haziran 2019 tarihinde http://bidb.meb.gov.tr/www/mill-egitim-bakanligi-bilisim-sistemleri-tanitim-videosu/icerik/72/?iframe=true&width=90%&height=90% adresinden erişilmiştir.

Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime*. Routledge.

Parlak Yorğancı, D. (2018). Çocukların sosyal medya kullanımlarına yönelik yetişkin tutumları üzerine nitel bir inceleme. *Abant Kültürel Araştırmalar Dergisi, 3*(5): 182-202.

Pusey, P. & Sadera, W.A. (2011). Cyberethics, cybersafety and cybersecurity: Preservice teacher knowledge, preparedness and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education, 28*(2), 82-88.

Rand Europe Report (2014). 26 Mayıs 2019 tarihinde www.rand.org adresinden erişilmiştir.

Rani, S. (2017). Cyber security awareness among Malaysian pre-university students. *Conference: 6th Global Summit of Education*, Kualalumpur, Malaysia.

Sabillon, R., Cano, J., Cavaller, V. & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6), 165-176.

Sağıroğlu, Ş. (2018). Siber güvenlik ve savunma: Önem, tanımlar, unsurlar ve önlemler. Şeref Sağıroğlu ve Mustafa Alkan (Ed.), *Siber Güvenlik ve Savunma, Farkındalık ve Caydırıcılık* içinde (21-45). Ankara: Grafiker Yayınları.

Semerci, A. (2016). Examining middle school students' views on text bullying. *Education and Information Technologies, 21*(6), 1807-1819.

STM (2018). 2018 Ocak-Mart dönemi siber tehdit durum raporu. 09.02.2019 tarihinde https://www.stm.com.tr/documents/file/Pdf/siber-tehdit-durum-raporu-ocak-mart-2018.pdf adresinden erişilmiştir.

Tekerek, M. & Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education, 2*(3), 61-70.

TrendMicro (2019). Türkiye' de en çok karşılaşılan beş siber saldırı çeşidi. 24 Nisan 2019 tarihinde http://usga.com.tr/turkiye-de-en-cok-karsilasilan-bes-siber-saldiri-cesidi/ adresinden erişilmiştir.

Türk Ceza Kanunu (2014). Türk Ceza Kanunu. http://www.mevzuat.gov.tr/MevzuatMetin/ 1.5.5237.doc

UNICEF (2017). Dünya çocuklarının durumu, dijital bir dünyada çocuklar. 29 Mayıs 2019 tarihinde http://www.unicef.org.tr/files/bilgimerkezi/doc/SOWC_2017_SUM_TR.pdf adresinden erişilmiştir.

Yenilmez, K. (2008). Open primary education school students' opinions about mathematics television programmes. *Turkish Online Journal of Distance Education, 9*(4), 176-189.

Yılmaz, E., Şahin, Y. L. & Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya Üniversitesi Eğitim Fakültesi Dergisi, 6/2*, 26-45.

Yiğit, M.F. & Seferoğlu, S.S. (2019). Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi, 15*(1), 186-215.